GIGABYTE™
TECHNOLOGY

GN-AP03GM

AirCruiser MIMO Access Point

User's Manual

www.gigabyte.com.tw
December 2005
Revision 1.0

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Change direction or location of antenna.
- Increase the distance between the equipment and the antenna.
- Connect this equipment with a socket different from the one connected with antenna
- Ask help from experienced audio/video technicians.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be install and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contents

Chapter 1 Introduction 4
Overview 4
Features 4
Package Contents 5
GN-AP03GM Rear Panel 5
Front Panel 6
Chapter 2 QUICK INSTALLATION 7
Hardware Requirements 7
System Requirements 7
Internet Configuration Requirements 7
Hardware installation 8
Assigning an IP address to your Access Point 9
Chapter 3 Configuration - Using AP Manager 12
Access Point Manager (AP Manager) 12
Install Access Point Manager 12
Using Access Point Manager 16
Uninstall AP Manager Utility 35
Chapter 4 Configuration - Using your Web-Browser 37
Using Web-based configuration 37
Chapter 5 Troubleshooting 47
Appendix A: Glossary 49
Appendix B: Specifications 51
Physical Interface 51
Specifications 51
Appendix C: Configuration of the PCs 53
TCP/IP Settings Under Windows 2000 53
TCP/IP Settings under Windows XP 55

Chapter 1 Introduction

Overview

The GN-AP03GM AirCruiser MIMO (Multi-Input & Multi-Output) Access Point includes several devices in one box. First, there's the Wireless Access Point, which lets you connect Wireless-G or Wireless-B devices to the network. There's also a built-in one port full-duplex 10/100 Ethernet port to connect your wired-Ethernet devices. Connect PCs directly, or daisy-chain out to more hubs and switches to create as big a network as you need. This product operates in 2.4 GHz frequency bands, providing fast (up to 54 Mbps) and secure (support WPA and WEP) connections to 802.11 b/g networks. GN-AP03GM overcomes environment multi-path effect by MIMO feature to keep stable wireless performance.

****** MIMO (multiple-in, multiple-out) takes advantage of multiplexing to increase wireless bandwidth and range. MIMO algorithms send information out over two or more antennas and the information is received via multiple antennas as well

Features

- Conforms to IEEE 802.11g specification.
- Support 64-bit /128-bit WEP encryption, WPA.
- Support DHCP client
- Support DHCP server
- Easy Web Management
- Web based Firmware upgrade
- MDI/MDIX Auto crossover detect

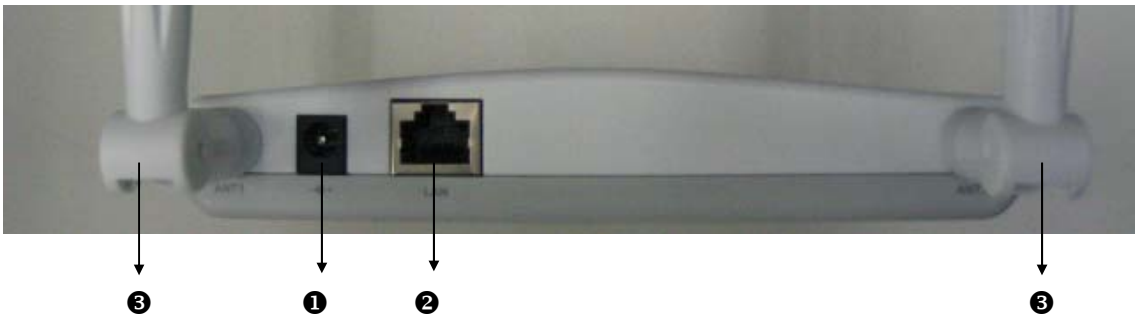
Package Contents

Before installation, please ensure the components are not damaged during the shipping. The package contents of the GN-AP03GM shall include:

- One GN-AP03GM AirCruiser MIMO Access Point
- One Power Adapter
- One installation CD contains AP Manager and User's Guide
- User's Guide
- One RJ-45 cable

If there are any missing or damaged parts, please contact your local distributor or dealer immediately. If a replacement unit is needed, return the device with the original packing material, otherwise the warranty will be voided.

GN-AP03GM Rear Panel



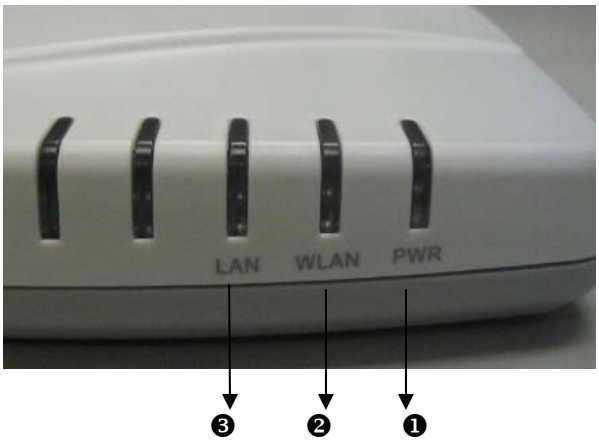
The AirCruiser MIMO Access Point's ports are located on the AP's rear panel and the antenna is located on the side panel.

❶ **Power Socket**
The power socket connects the GN-AP03GM to the power adapter.

❷ **Ethernet LAN Port**
RJ-45, Auto-sensing and Auto-MDI/MDIX for 10/100M Ethernet LAN connection.

❸ **Antenna**
Dipole-type high gain removable 2.4 GHz antenna

Front Panel



LED's

The AirCruiser MIMO Access Point's LED displays information about the AP's status.

❶ **Power on** (Green LED)

When the LED is on, the power is supplied to GN-AP03GM.

Note: When you change the settings and save them, the power LED will be temporarily off.

❷ **WLAN** (Green)

On	Wireless system ready
Flashing	Data is being transmitted wirelessly.

❸ **LAN** (Green)

On	LAN port has detected a link with a 10/100 Mbps device.
Flashing	Data is being transmitted wirelessly.

Chapter 2 QUICK INSTALLATION

Hardware Requirements

Suggested Computer specifications for AirCruiser MIMO Access Point installation:

- A PC or Macintosh Computer
- One installed 802.11b/g wireless PCI LAN adaptor
- An Ethernet router or hub
- RJ-45 Ethernet patch cable

Minimum Computer specifications for AirCruiser MIMO Access Point installation:

- A PC or Macintosh Computer
- An Ethernet router or hub
- RJ-45 Ethernet patch cable

System Requirements

Operating System: Works under Windows, Macintosh or Linux operating systems. If wishing to activate AP Manager, it is strongly suggested that you use either Windows XP or 2000 OS.

Internet Configuration Requirements

To connect AP Manager with AirCruiser MIMO Access Point, please set up the following parameters for TCP/IP configuration:

Static IP Address: 192.168.1.x. Where ‘x’ is between 2 – 253.
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254

Hardware installation

Follow the steps below when installing your Access Point(s). (hereafter refered to as APs)

Connecting your AP for initial configuration may be done by wired or wirelessly, however it is STRONGLY SUGGESTED you follow "Connecting with wired Ethernet" since this method you will not have to deal with the extra steps of creating a wireless connection.

Before you setup, please keep the following in mind when placing your AP.

Select a suitable location to install the AP. Assure also that the location is **away** from any interfering radio signals from devices such as microwave ovens, garage door openers, vacuum cleaning devices, etc. Please also operate the AP in a cool dry place, away from direct sunlight.

Position the AP appropriately. Signal strength is greatly dependent on your well placed AP. Generally, a centralized area with 360° clear line of sight is the best location with the antenna in a high position to allow optimal propagation of the signal. **The location of the AP greatly influences the signal reception.**

◆ Making a Wired Connection (Highly recommended method for first time setup)

Step 1 Turn off all the hardware devices in your network, including the router/hub by unplugging their power supply.

Step 2 Connect the Ethernet cable of your router/hub to the LAN port of the GN-AP03GM.

Step 3 Connect one end of an Ethernet LAN cable to one of the LAN ports on your router/hub, and the other end to an Ethernet port of your computer.

Step 4 Plug the power adapter cord into the AP's power jack and then plug the power adapter into a power outlet.

Step 5 Turn on your router/hub. After verifying all the connections, proceed to **Chapter 4 – Configuring the PCs**.

◆ Making a Wireless Connection

Step 1 Turn off all the hardware devices in your network, including the router/hub by unplugging their power supply.

Step 2 Connect the Ethernet cable of your router/hub to the LAN port of the GN-AP03GM.

Step 3 Plug the power adapter cord into the AP's power jack and then plug the power adapter into a power outlet.

Step 4 Turn on your router/hub. After verifying all the connections, proceed to **Chapter 4 – Configuring the PCs**

Note: If using a wireless connection, please refer to the user manual of the wireless adapter to install. The SSID of the wireless adapter and the GN-AP03GM should be identical. The default SSID assigned to the GN-AP03GM is **GIGABYTE**. (WARNING: The SSID field is case sensitive, so for example "a" is different from "A").

For typical home use, the range of signal reception should not be an issue. In case of weak (or no) signal where the wireless LAN is used, please consider placing the AP with clear line of sight (no walls/obstructions) between the computer and a wireless adaptor. Additional APs can be connected for rooms out of the coverage to build up a better cloud of reception.

Assigning an IP address to your Access Point

Your AP will be identified on the network by its IP address. There are two ways of assigning it: Manually assign, or use DHCP to automatically assign one for you (preferred).

◆ Method 1: Manually assign Static IP address

If DHCP is **not used** on the network, the AP can be set up via a direct connection to the computer.

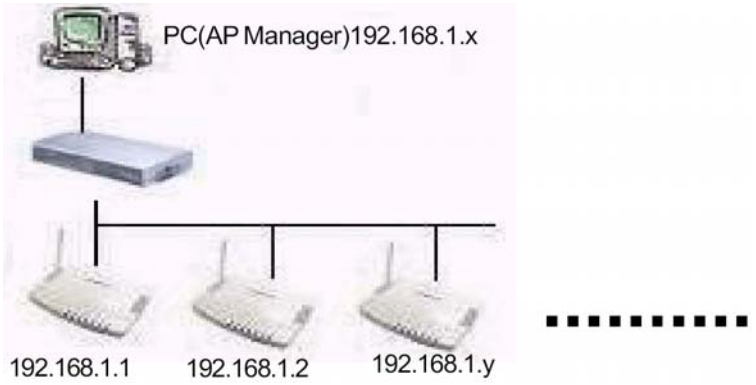
PC (AP Manager) 192.168.1.x

Access Point
192.168.1.1 (Default)

1. You must assign a static IP address to the computer. The **Subnet** must be the same for the computers and AP. The default IP address of the AP is 192.168.1.1 and the Subnet Mask is 255.255.255.0. For example, you can enter an IP address of 192.168.1.20 (if not assigned to other network equipments) and an Subnet Mask of 255.255.255.0.

   Note: For further instructions regarding to this step, please refer to **Appendix C**, **Computer Configuration**.

2. Please connect APs in turn and assign a static IP's to each AP, incrementing each additional AP address by one in the least significant octet. For example, 192.168.1.**2** then 192.168.1.**3**, etc…



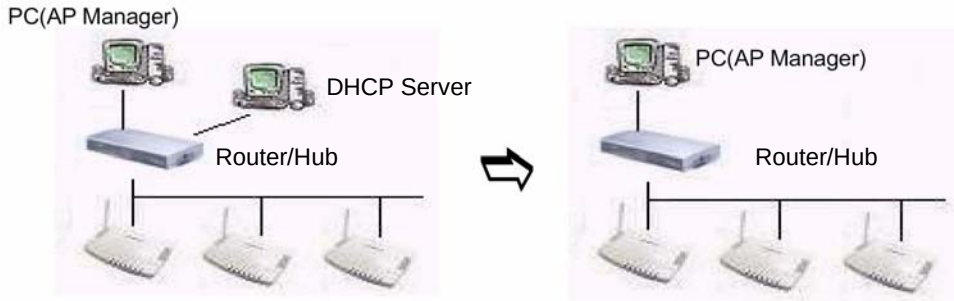
3. Please make sure an each AP has a **unique IP address**.

4. After setting all IP addresses successfully, you can use AP manager to control / monitor each AP.

◆ Method 2: Using DHCP to automatically assign IP

In this method, we will use DHCP server will do the work of dynamically assigning IP addresses for all APs – assigning each AP an exclusive IP address. After set up, just remove or disable the DHCP server. You can search all APs with AP Manager and assign a static IP address for additionally added AP's.

Note: Please assure that all APs are in the **same Subnet**.



<u>Obtain an IP address automatically – DHCP server is enabled</u>

If a DHCP server is used on the network, it can connect to APs and the Gigabyte AP Manager through a router or hub. You should set the IP address of AP as "Obtain an IP address automatically". DHCP will assign an IP address to the AP. The Subnet must be the same for the PC(AP Manager) and AP. Or, you can set

the PC (AP Manager) as “Obtain an IP address automatically” and assign IPs with the same DHCP.

Note: You can also use Gigabyte AP Manager to connect APs through a Wireless LAN adaptor.

Chapter 3 Configuration - Using AP Manager

There are two methods of setting up the AP: Using the web-based configuration, or using Gigabyte's AP Manager Utility. **AP Manager is only used for Gigabyte Access Points.** This Chapter will introduce how to set up APs through AP Manager.

Access Point Manager (AP Manager)

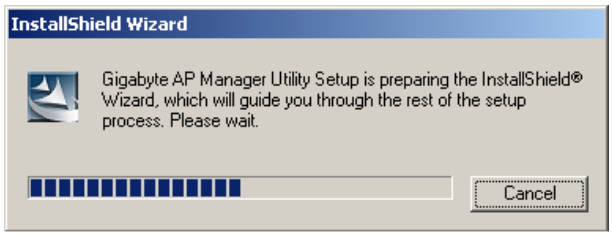
Note: 1. Setting up the AP may be done wirelessly or with a wired connection, however we will assume you are using a wired connection for initial setup.
2. You are also suggested to disable any firewall before setting up the Wireless LAN Access Point with AP Manager utility.

Install Access Point Manager

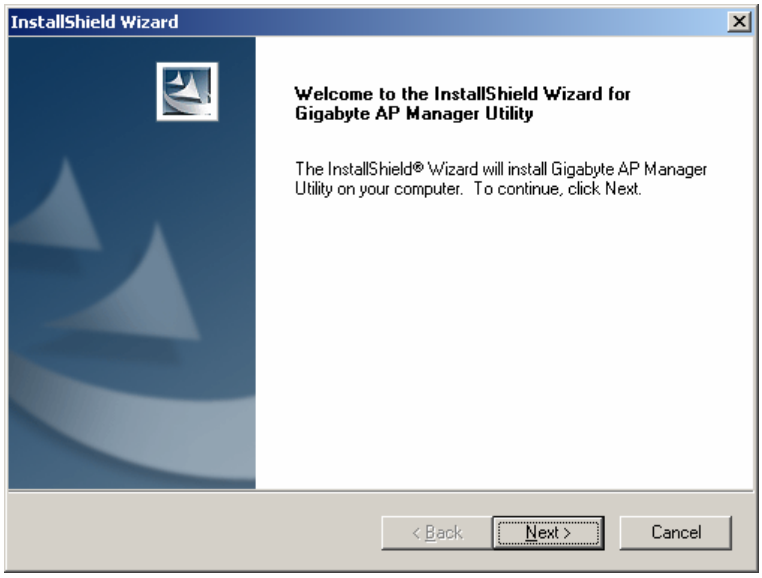
Please install "Gigabyte AP Manager" in Windows by following the steps below.

Step 1: Insert the Installation CD into your CD-ROM drive and click **"Install Gigabyte AP Manager"**.

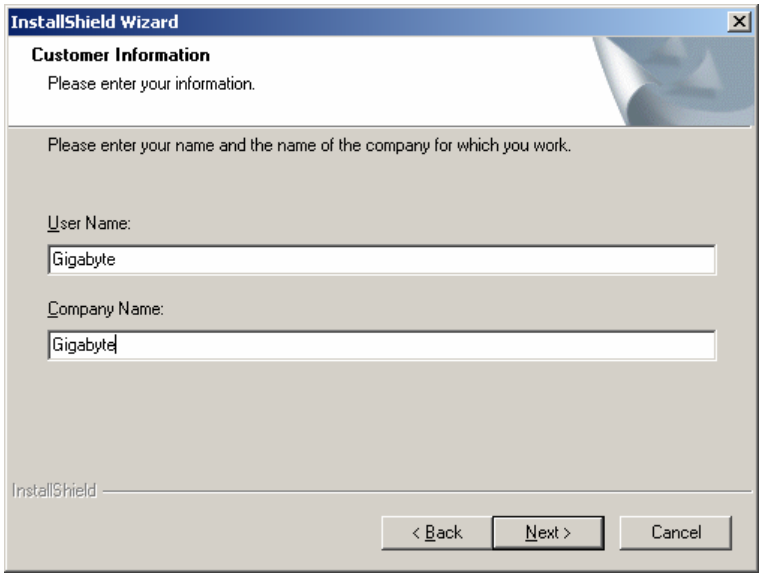
Step 2: Wait a moment as the Install Shield wizard starts.


InstallShield Wizard
Gigabyte AP Manager Utility Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

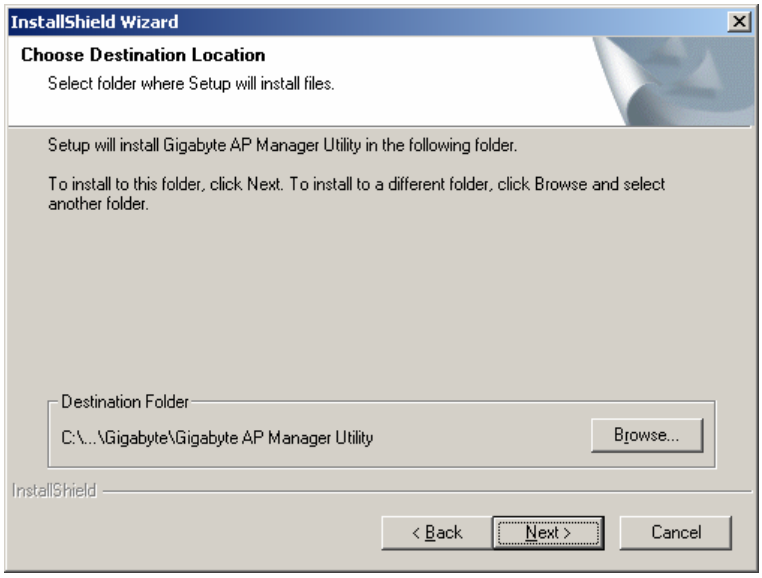
Step 3: Click **"Next"** to proceed through the wizard.


InstallShield Wizard
Welcome to the InstallShield Wizard for Gigabyte AP Manager Utility
The InstallShield® Wizard will install Gigabyte AP Manager Utility on your computer. To continue, click Next.
< Back
Next >
Cancel

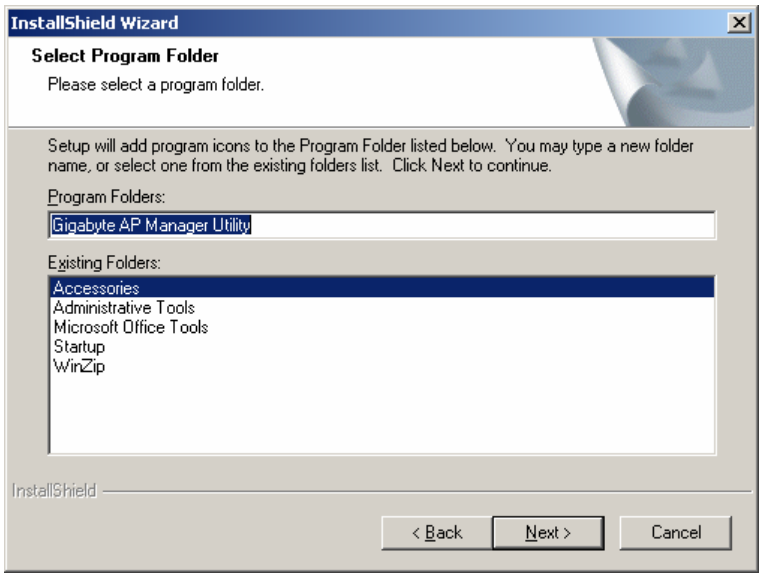
Step 4: Enter users name and company name then click **"Next"**.



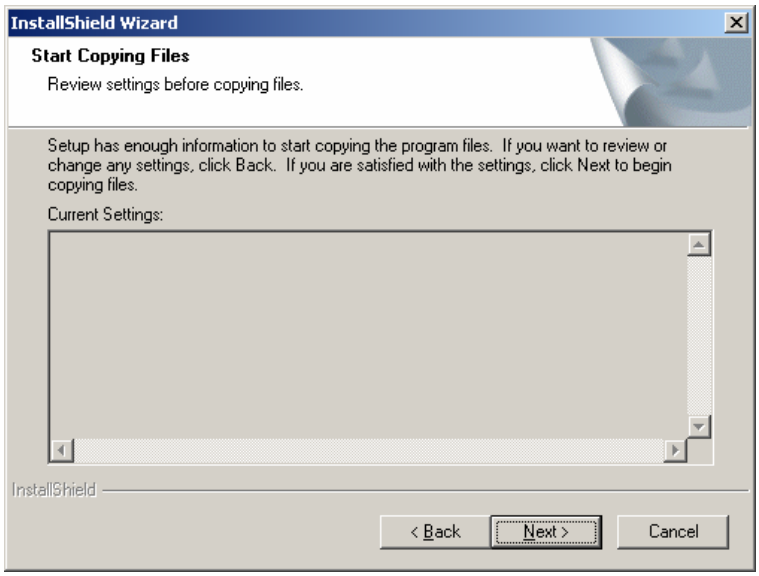
Step 5: Choose Destination Location. Click **"Next"** to accept default directory or click **"Browse"** to specify a different install directory.


InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install Gigabyte AP Manager Utility in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\Gigabyte\Gigabyte AP Manager Utility
Browse...
InstallShield
< Back
Next >
Cancel

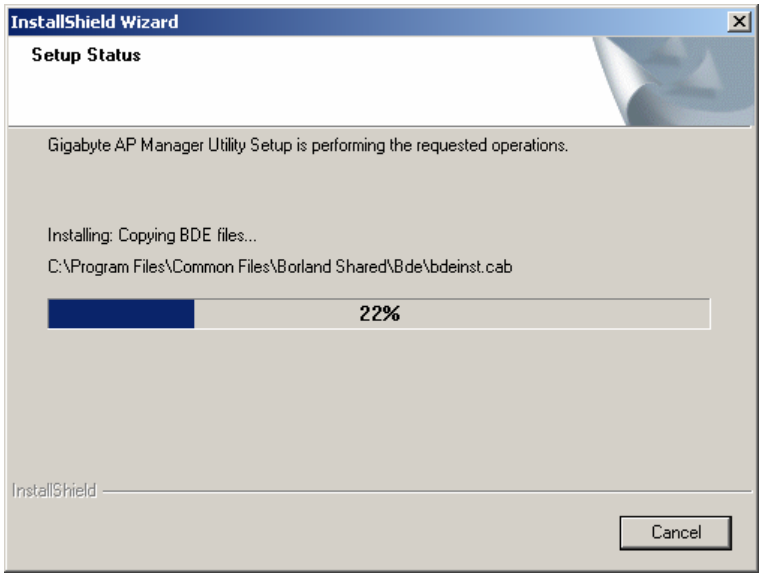
Step 6: Create a Program Folder. Click **"Next"**.


InstallShield Wizard
Select Program Folder
Please select a program folder.
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.
Program Folders:
Gigabyte AP Manager Utility
Existing Folders:
Accessories
Administrative Tools
Microsoft Office Tools
Startup
WinZip
InstallShield
< Back
Next >
Cancel

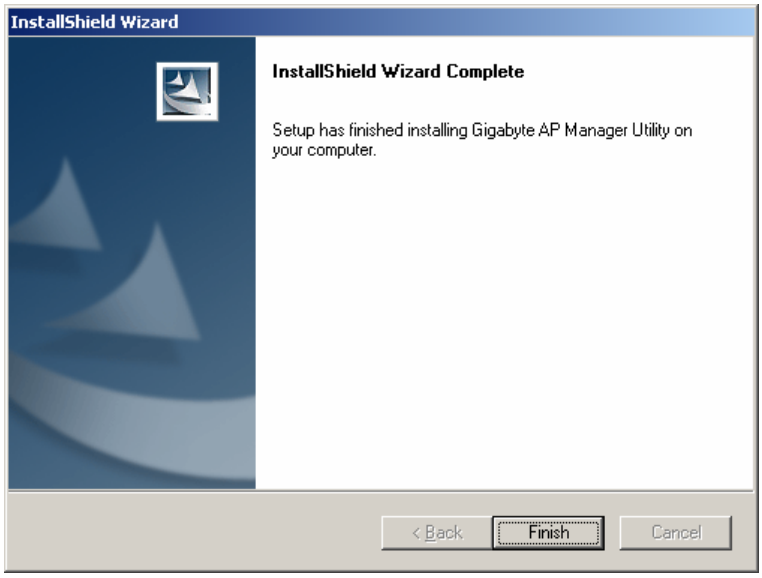
Step 7: Copy program files to your Hard Drive. Click **"Next"**.


InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
InstallShield
< Back
Next >
Cancel

Step 8: Setup status will display progress bar. Wait a moment.



Step 9: Click **"Finish"** to complete the installation.

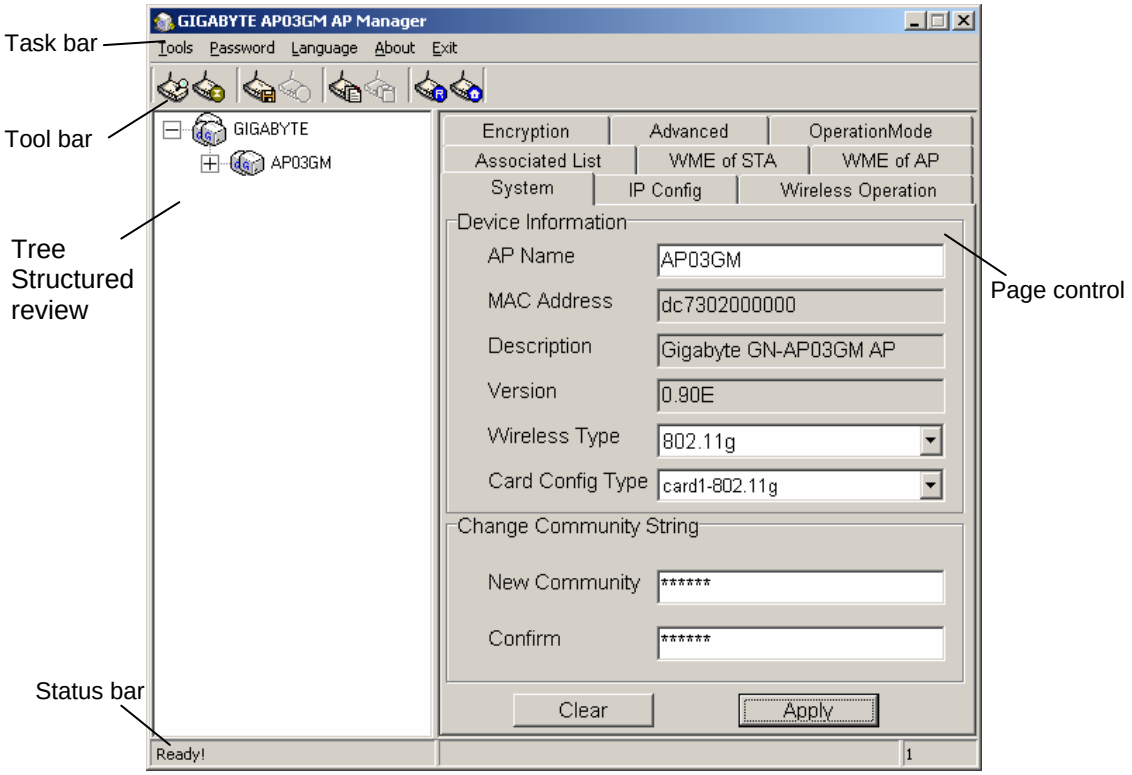


Using Access Point Manager

From the Windows Start button, click **Start > Programs > Gigabyte AP Manager Utility/Gigabyte AP Manager** to launch the Gigabyte AP Manager.

Enter the default password “admin” and click “OK”.

When you open Gigabyte AP Manager, it will automatically search for AP in the same Subnet. You can also double click the icon in the Tool bar to manually search for any AP.



The Task Bar

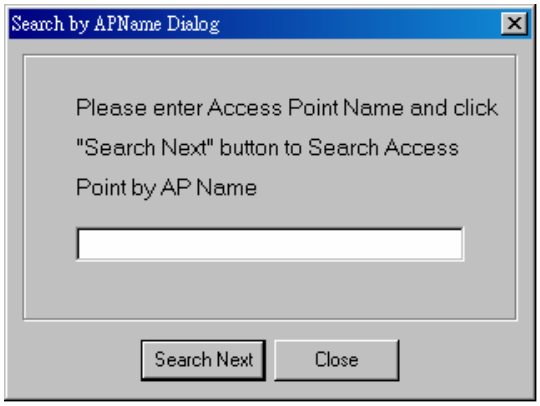
Tool: Allows you to **"Search"** AP and **"Connect to AP by IP"** through ESSID, AP name, MAC address and IP address. It also allows you to **"Save"** and **"Load"** AP configurations and to **"Copy"** and **"Paste"** configurations on the current page. Other functions include **"System Reboot"** and **"Load Default"**.

Password: Allows you to change password for AP Manager and set SNMP strip.

Help: On-line help and AP Manager version.

Exit: Exit the AP Manager.

Note: When you search an AP via an AP name (Tools->Search->By AP Name), you may click **"Search Next"** to find APs with the same name.


Search by APName Dialog
Please enter Access Point Name and click "Search Next" button to Search Access Point by AP Name
Search Next
Close

The Tool bar

Find Access Point

Find all APs in the same Subnet.

Save AP Configuration

Save AP configurations in a temporary file.

Page Copy

Copy configuration for current page.

Page Paste

Paste copied content to the current page. (You may paste the settings from AP1 to AP2 on the same bar tab.)

System Reboot

Reboot AP.

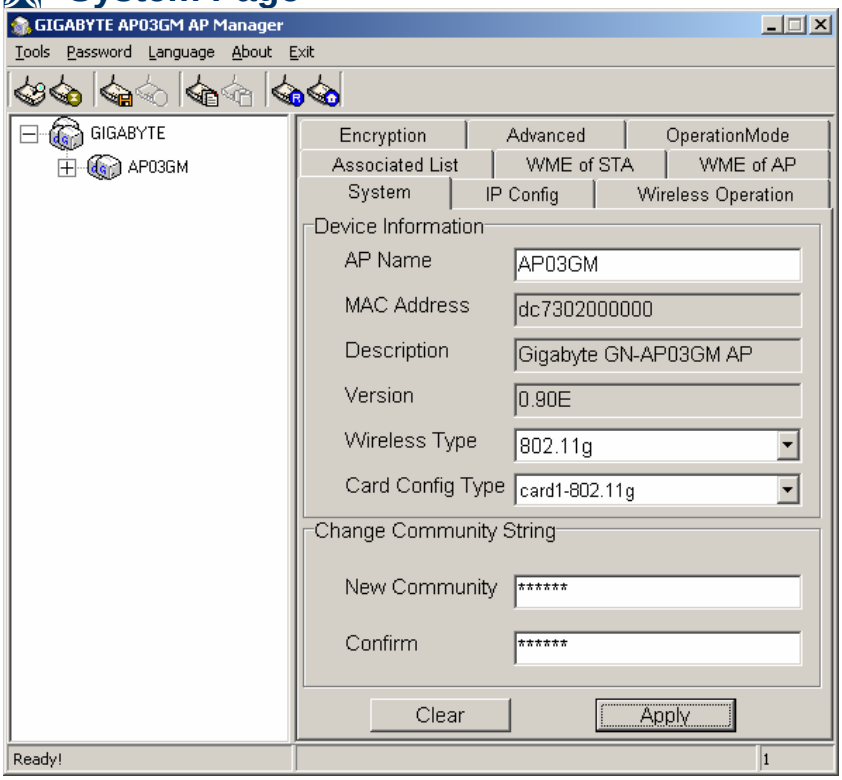
Load Default

Load default values for AP.

Connect to AP by IP

If you want to manage APs on different Subnets, use this function and enter IP.

System Page



The system page main topics are **"Device Information"** and **"Change Community String"**.

- ***Device Information***

  "Device Information" includes AP names, MAC addresses, description, version, wireless type and card configuration type.

  1. You may change "AP name" to any name in order to specify the AP.
  2. You may select your desired wireless protocol from "Wireless Type".
  3. You may select desired wireless LAN card from "Card Config Type".

- ***Change Community String***

  The community string must be the same for AP Manager and APs; as AP Manager only monitors AP with the same community string. This is a security measure to prevent other AP Mangers from accessing and managing your APs. After changing strings, you have to complete the following steps for the consistency of community strings.

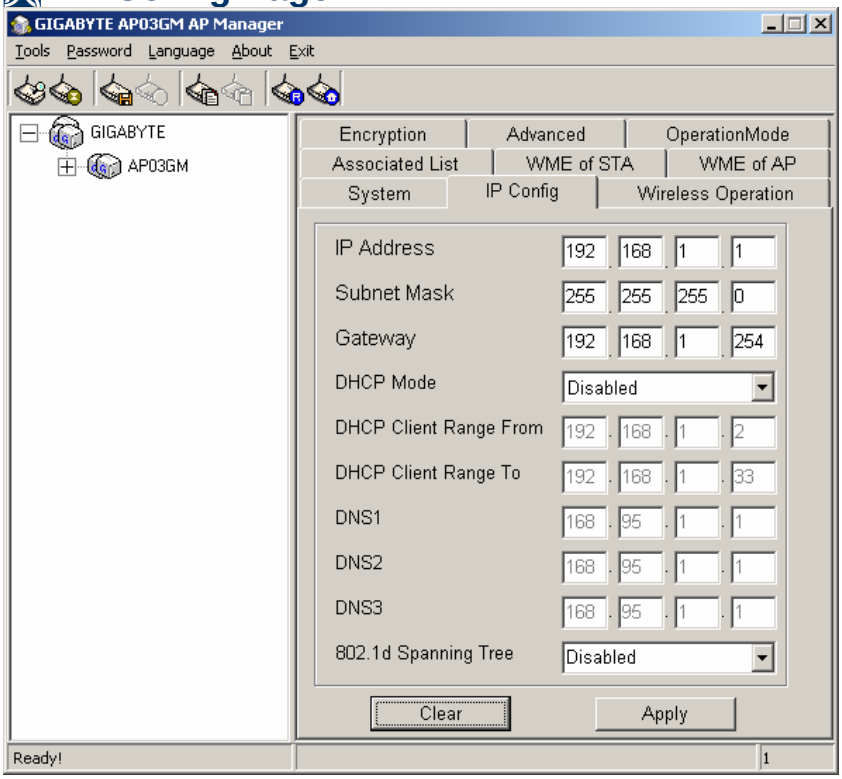
  1. Go to **Task Bar -> Password -> Set Community String** and set the community string for AP Manager.
  2. Don't forget the community string. We suggest you write it down and keep it handy.

If you do ever forget the community string, you'll need to press the "INIT" button on the underside of the AP which will restore all factory default values (including the community string).

Note:

SNMP community string defines the relationship between SNMP AP Manager and agent systems (all APs) and controls the access of AP Manager to APs with password. The default value is “public”. Go to **Task Bar -> Password -> Set Commuinity String** and change the community string for AP Manager.

IP Config Page



Set the IP parameters for APs in the “IP Configure” tab.

- ***IP Address***
  Assign an IP address to the AP with this option. The default IP address is 192.168.1.1. Please make sure the assigned IP address is exclusive for the AP.

- ***Subnet Mask***
  Assign a Subnet Mask for an AP. The default Subnet Mask is 255.255.255.0.

- ***Gateway***
  Enter the IP address for the default router. The default gateway is 192.168.1.254.

After changing the IP address for AP, please change the PC’s IP address (AP Manager) so that both have the same Subnet Mask. Then, click the **“Find Access Point”** icon and AP Manager willl find APs on the network.

- ***DHCP Mode***
  Four options are available here: “Disabled”, “Client Enabled” , “Server Enabled” and “Auto”. The default setting is “Auto”.

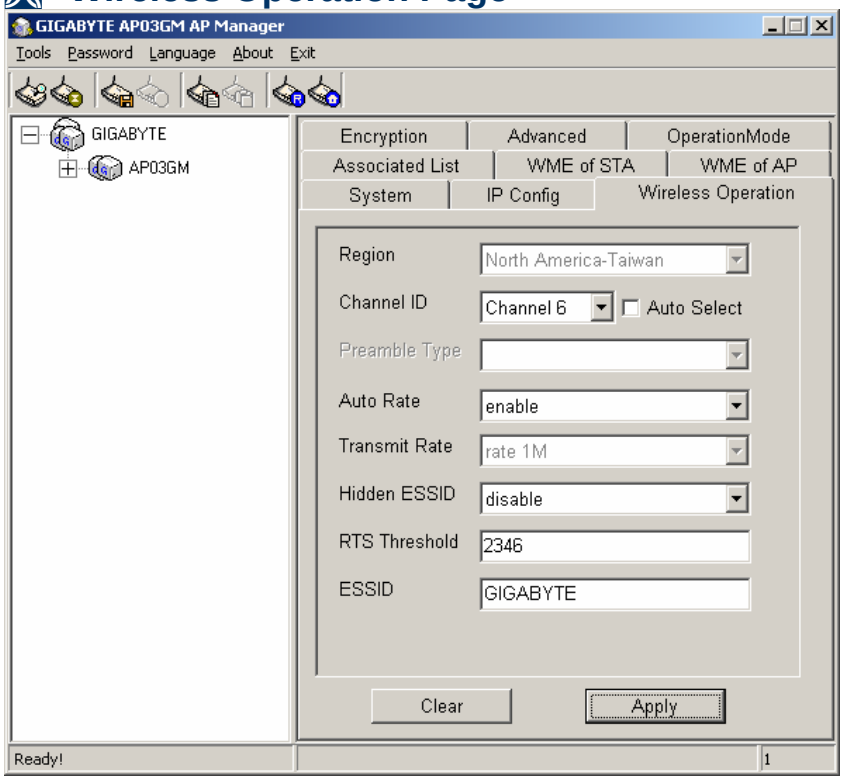
  If you want to obtain IP addresses from a DHCP server, select **“Client Enabled”**. To use an AP as a DHCP server and assign a dynamic IP address automatically on the network, select **“Server Enabled”**. If you are not sure DHCP server is available on the network and wish to use an AP as DHCP server, please select “Auto”.

- ***DHCP Client Range & DNS***
  When “Server Enabled” is selected, please enter the range of your IP addresses and DNS. DNS information is provided by your ISP.

- ***802.1d Spanning Tree***
  When the 802.1d Spanning Tree function is enabled, the short circuit problems, loops and path redundancy among multiple APs or routers in the network can be avoided. It also comes with some overhead, and since there probably wont be many AP’s or rotuers in your network, the default value is “Disable”.

Confirm your desired settings and press **“Apply”** button to save the settings in the AP.

Wireless Operation Page



The wireless equipment still can operate smoothly with no changes made for any options on this page.

- ***Region***

  In that different regions have different open channel regulations; please check whether the default value for the region is suitable for your local area. In case of incompatibility, please contact your local distributor or authorized reseller immediately.

- ***Channel ID***

  Please choose the channel for best performance. Normally, no change is needed. The default value is "Auto" and will be detected automatically by the system.

- ***Transmit Rate***

  You can select the transmission speeds of 6M, 9M, 12M, 18M, 24M, 36M, 48M and 54M based on your needs. The default setting is **"54 M"**. The **"Transmit Rate"** function is disabled while **"Auto Rate"** is enabled.

Note: The standard transmission speeds of 802.11b are are 11M, 5.5M, 2M and 1M.

- ***Auto Rate***

  You can select **"Enable"** or **"Disable"** in this option. The default setting is **Enable**.

  Enable When **"Enable"** is selected, the transmit rate will give you the highest negotiation rate possible. It does this by first attempting to negotiate at 54Mbps, and then systematically throttle down to the next highest rate available. The range of automatic change is based on the **"Transmit Rate"**.

  Disable The transmission speed does not change automatically and is defined by **"Transmit Rate"**

  Transmit rates:
  54M: range from 6M, 9M, 12M, 18M, 24M, 36M, 48M to 54M
  48M: range from 6M, 9M, 12M, 18M, 24M, 36M to 48M
  36M: range from 6M, 9M, 12M, 18M, 24M to 36M
  24M: range from 6M, 9M, 12M, 18M to 24M
  18M: range from 6M, 9M, 12M to 18M
  12M: range from 6M, 9M to 12M
  6M: No automatic change is available. Transmission speed is fixed to 6M.

- ***Hidden ESSID***

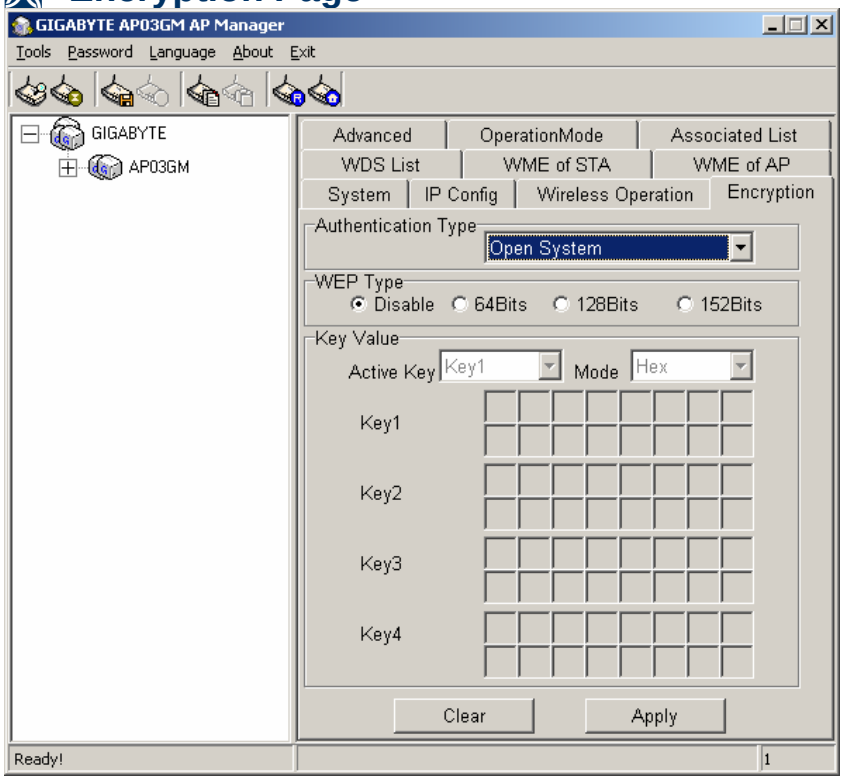
  This setting enables you to hide ESSID, which is needed by the users to connect to AP. Hiding your APs ESSID is a security measure sometimes used in order to prevent strangers from seeing the existence of your wireless access point, thereby attempting to gain access too it. The default setting is **"Disable"**.

- ***RTS Threshold***
  The default value of “2346” should not be changed. However, in case of inconsistent data flow, adjustment the value to a lower number and retry. Enter a value within the range 0~2346 for the port. RTS (Request To Send) is a function, requesting permission to transmit signals. RTS is a collision avoidance method used by all 802.11b wireless networking devices. In most cases you will not need to activate or administer RTS. Generally, RTS only needs to be configured if you find yourself in an Infrastructure environment where all nodes are in range of the Access Point but may be out of range of each other.

- ***ESSID***
  ESSID or SSID refers to AP names in the wireless network. You should set the **same** ESSID name for all APs clients to dynamically roam among APs. The SSID is up to 32 ASCII characters in length and case sensitive (ie. Letters in upper case **“A~Z”** and lower case **“a~z”** are unique).

Confirm your setting and click **“Apply”** button to save the settings in APs.

Encryption Page



In this page you may secure your network by using WEP (Wired Equivalent Privacy) “802.11b/g standard of 64/128 bytes”. Select Disable to disable WEP encryption. When “64bits” or “128bits” is selected, the data transmitted will be encrypted and unauthorized users will be prevented from accessing the wireless network.

- ***Authentication Type***
  You may select from “Open System”, “Shared Key”, “Both”, “WPA” and “WPA-PSK”. The default value of authentication type is “Shared Key”.

  Open System The sender and the recipient do not share a key. Each party generates its own shared key and asks the receiver to accept the (usually randomly) key. Once accepted, this key is used for a short time only, and then a new key is generated.

  Shared Key The sender and the recipient share a key.

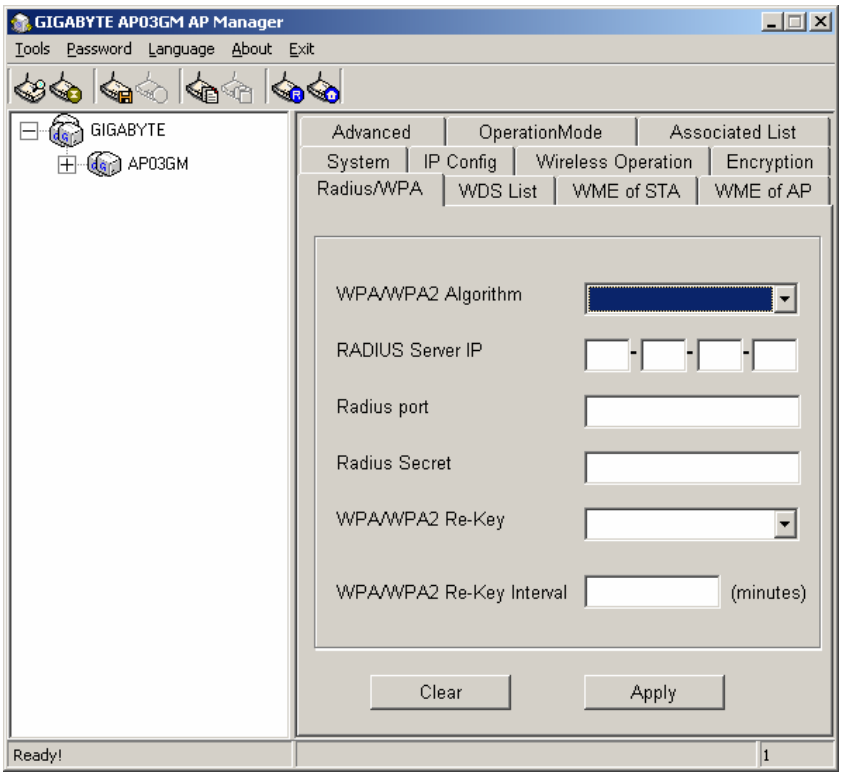
  If you select **“Shared Key” or **“Both”**, in the WEP option, **“Disable”**, will not be avaiable.

  WPA/WPA2 If you have used Wi-Fi for a while, you may be familiar with 802.1x Authentication Protocol, which allows users to authenticate the wireless network via RADIUS server. 802.1x Authentication Protocol is an option in standard Wi-Fi but a must for Wi-Fi Protected Access™(WPA). If a RADIUS server is not available in your environment,

regardless of the needs of 802.1x, you can use WPA. As another option for RADIUS server, WPA supports pre-shared key.

WPA/WPA2-PSK WPA Pre-shared key. Traditional WEP has an inconvenient method to change encrypted keys. Even you change encrypted keys; you still can not select all APs and wireless LAN adapter while changing encrypted keys. The manual re-keying which is necessary with WEP is a tedious manual process and is completely impractical for large organizations. After all, the instant you re-key an access point, none of the clients will be able to access it until they are also re-keyed.
But with WPA, the re-keying of global encryption keys is all that is necessary. In the case of unicast traffic, the encryption key is changed after every frame using Temporary Key Integrity Protocol (TKIP). This protocol allows key changes to occur on a frame-by-frame basis and to be automatically synchronized between the access point and the wireless client. Global re-keying works by advertising the new keys to wireless clients.

When you select WPA/WPA2 authentication type, a window for RADIUS settings will be displayed as follows. Please note, IP configuration shall be set as fixed IP address and DHCP mode as “disabled” when WPA/WPA2 authentication type is selected.



WPA/WPA2 Algorithm Two settings are possible: TKIP or AES.

RADIUS server IP Please assign an IP address to the primary RADIUS server (authentication server).

RADIUS Port The setting range is 1~65536 and the default value is 1812.

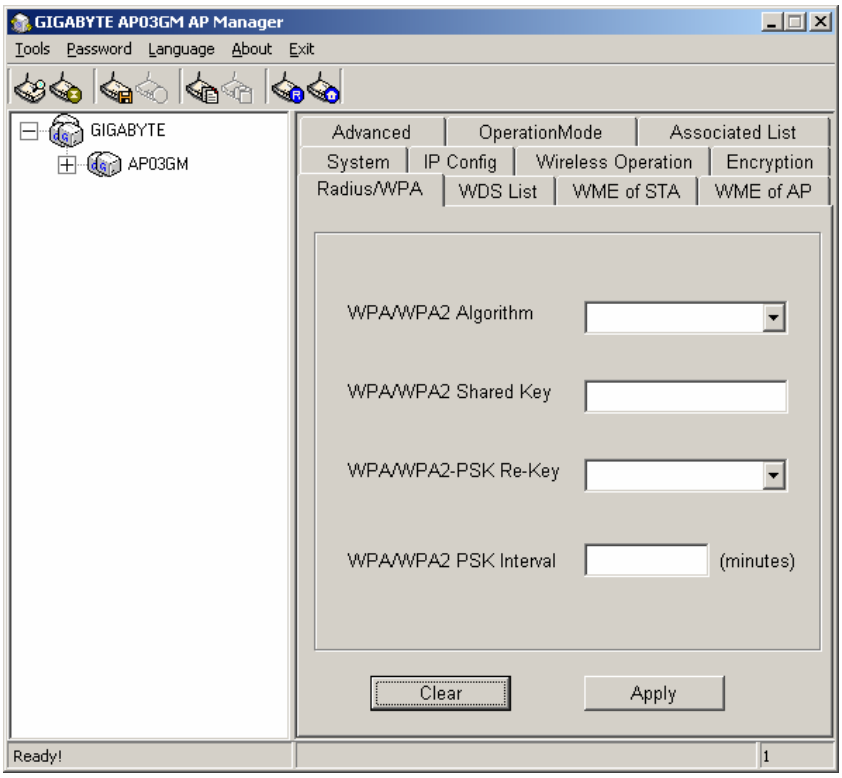
RADIUS secret The secret phrase can be up to 256 characters.

WPA/WPA2 Re-Key Under this option two setting are possible: “enable” or “disable”. The default value is “enable”.

WPA/WPA2 Re-Key Interval Enter a value for re-key interval (unit: sec).

Verify the desired settings and then click the **“Apply”** button to set the value in the access point.

When you select WPA/WPA2-PSK authentication type, the primary RADIUS settings window will displayed as follows.



WPA/WPA2 Algorithm Two settings are possible: TKIP or AES.

WPA/WPA2 Shared Key This phrase can be up to 256 characters.

WPA/WPA2-PSK Re-Keying Under this option two setting are possible: “enable” or “disable”. The default value is

"enable".

WPA/WPA2 PSK Interval Enter a value for re-key interval (unit: minutes).

Verify the desired settings and then click the **"Apply"** button to set the value in the access point.

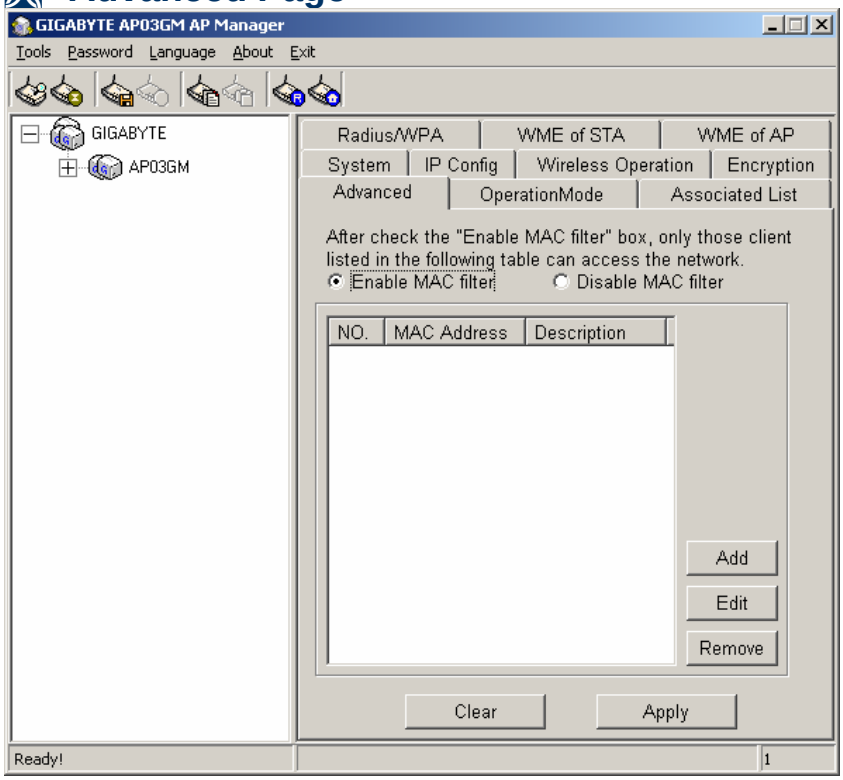
64 (40) Bits / 128 (104) Bits

There are three levels of encryption 64 bits, 128 bits and 152 bits. The 64 bits encryption is referenced as a lower level encryption. The 152 bits encryption is referenced as a higher level encryption.

The 64 bits WEP encryption use 40 bits as a secret key, which can controlled by user, and 24 bits as the initialize vector, which user can not control. These two portions plus together is 64 bits encryption. Some other vendor product might refer as 40 bits encryption. It is the same thing.

The 128 bits WEP encryption use 104 bits as a secret key, which can controlled by user, and 24 bits as the initialize vector, which user can not control. These two portions plus together is 128 bits encryption. Some other vendor product might refer as 104 bits encryption. It is the same thing.

Advanced Page



To enhance the security of the wireless network, this AP provides MAC address filtering mechanism to prevent the unauthorized access from specific physical network addresses. To invoke, check “Enable MAC filter” and key into the MAC address table those MAC address you wish to allow connection to this AP.

- ***Enable MAC filter***
  Choose the **“Enable MAC filter”** option, which only allows Network Interfaces of specified MAC addresses which you enter into the authorized MAC table. Click the **“Add”** button to add more MAC addresses or **“Remove”** to delete MAC addresses from the authorized MAC addresses table. You may **“Edit”** existing MAC address in this table as well.

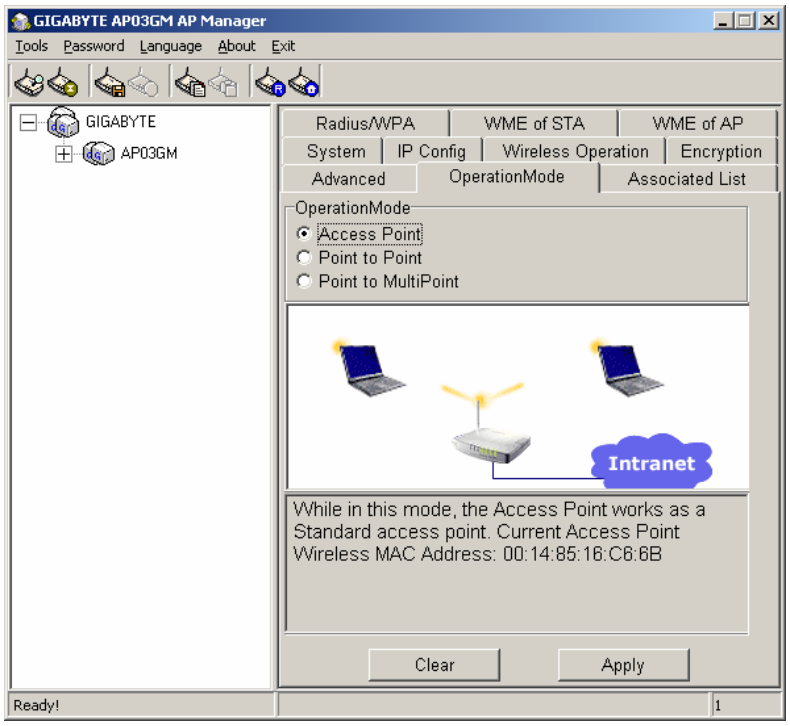
- ***Disable MAC filter***
  The default setting is **“**Disable MAC filter”. All Network Interfaces have access to the AP when MAC filter is disabled.

Verify the desired setting and then click the **“Apply”** button to set the value into access point.

WDS Operation Mode

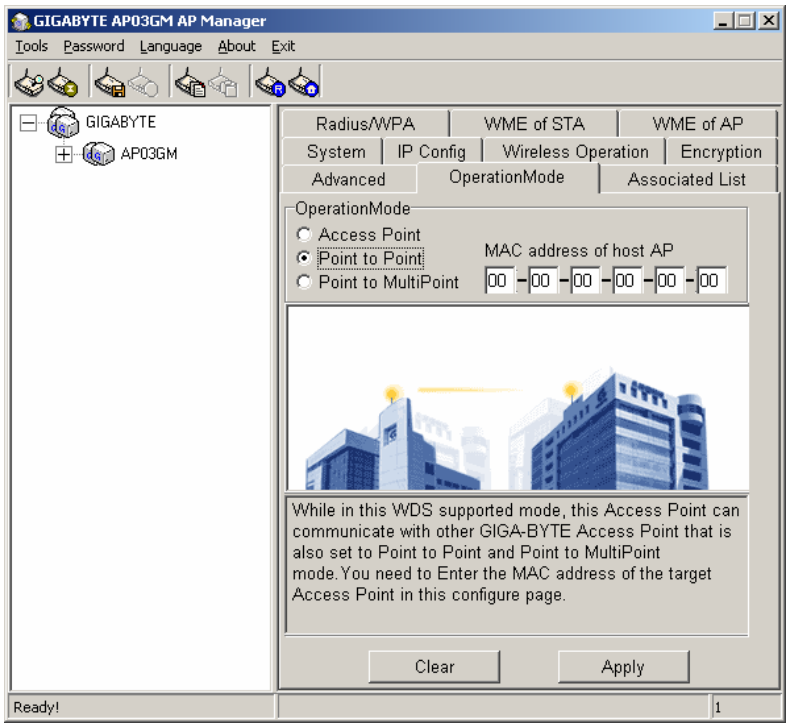
The Access Point supports three operation modes: “Access Point”, “Point to Point” and “Point to Multi-Point”. The default operation mode is “Access Point”.

Access Point



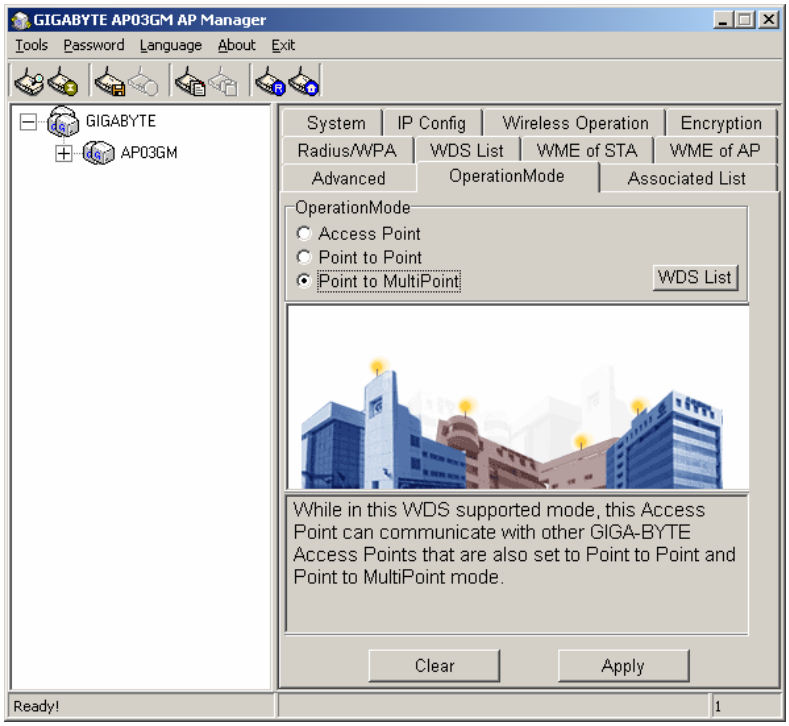
The operation mode is set to **“Access Point”** by default. This allows connection of your PC to most wired networks. In most cases, no configuration setting changes are necessary.

Point to Point

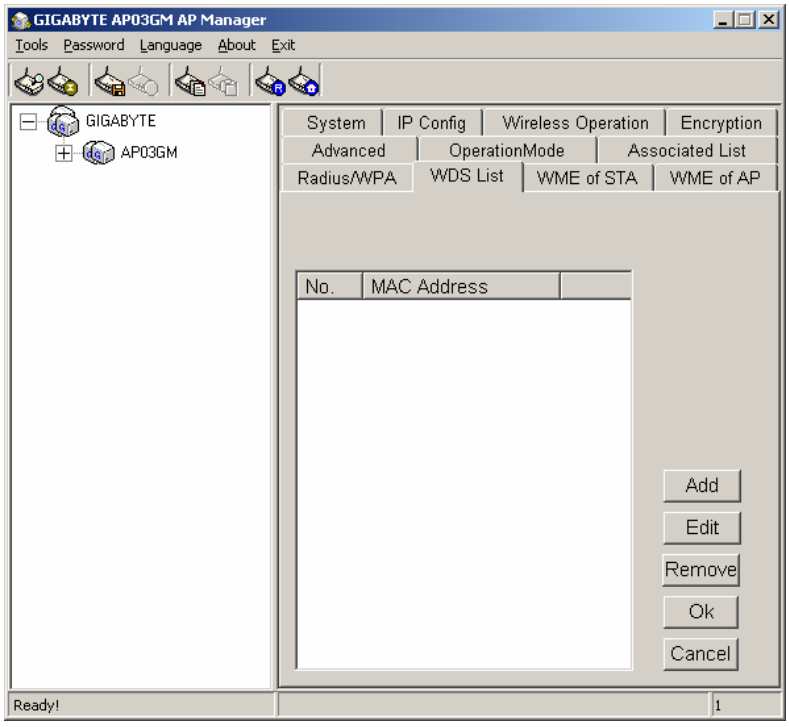

GIGABYTE AP03GM AP Manager
Tools Password Language About Exit
GIGABYTE
AP03GM
Radius/WPA
WME of STA
WME of AP
System
IP Config
Wireless Operation
Encryption
Advanced
OperationMode
Associated List
OperationMode
Access Point
Point to Point
Point to MultiPoint
MAC address of host AP
00 - 00 - 00 - 00 - 00 - 00
While in this WDS supported mode, this Access Point can communicate with other GIGA-BYTE Access Point that is also set to Point to Point and Point to MultiPoint mode. You need to Enter the MAC address of the target Access Point in this configure page.
Clear
Apply
Ready!

Only one Access Point can be assigned to connect with WDS in the “Point to Point” mode.
In this WDS supported mode, the Access Point can communicate with other Gigabyte Access Point that is also set to “Point to Point” mode. You have to enter the MAC address of the host AP.

Point to Multi-Point Mode

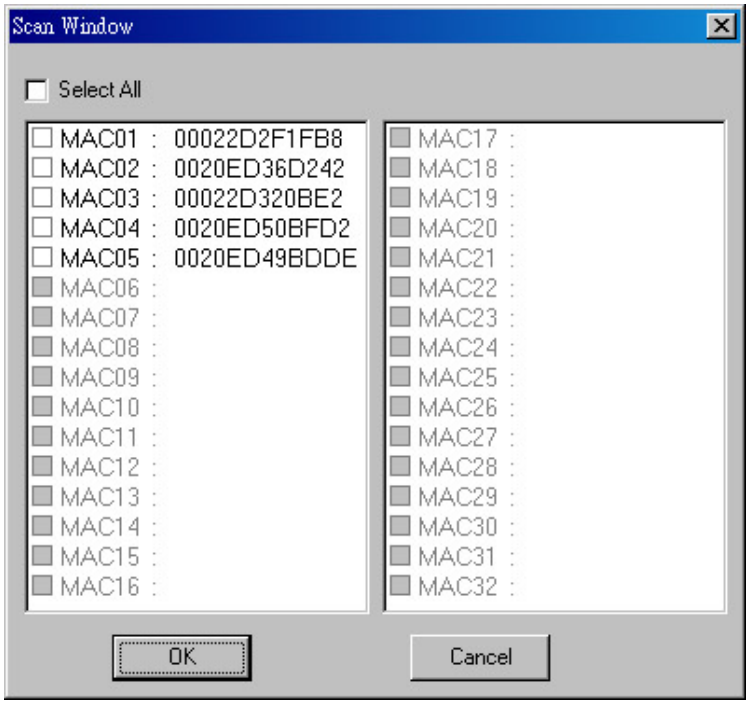

GIGABYTE AP03GM AP Manager
Tools Password Language About Exit
GIGABYTE
AP03GM
System IP Config Wireless Operation Encryption
Radius/WPA WDS List WME of STA WME of AP
Advanced OperationMode Associated List
OperationMode
Access Point
Point to Point
Point to MultiPoint
WDS List
While in this WDS supported mode, this Access Point can communicate with other GIGA-BYTE Access Points that are also set to Point to Point and Point to MultiPoint mode.
Clear
Apply
Ready!

Up to 8 Access Points can be set to connect through WDS list in “Point to MultiPoint”. In this supported WDS mode, the Access Point can communicate with other Gigabyte Access Points that are also set to “Point to Multi-Point” mode.

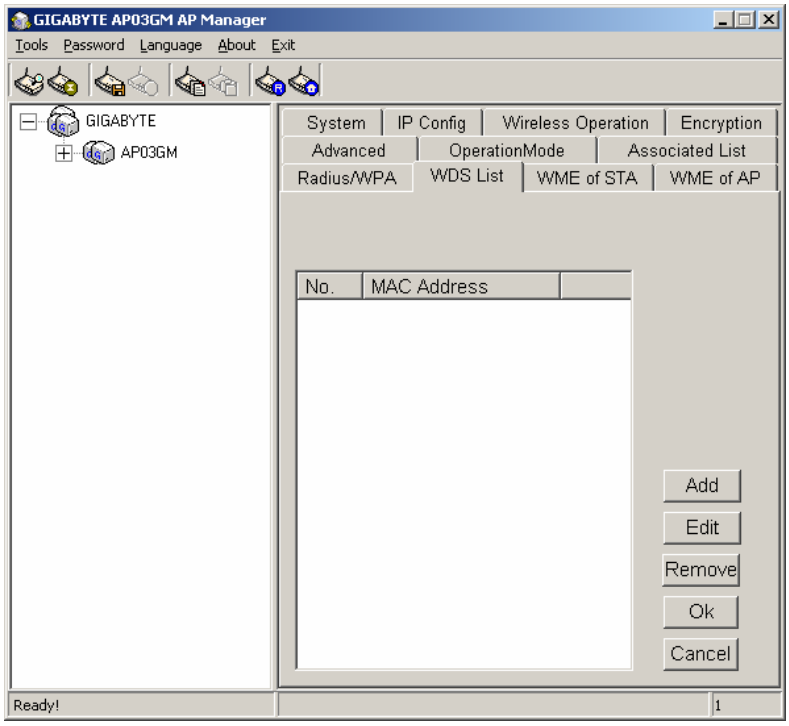


Click the “**WDS List**” tab to enter the “WDS List” page.

Note: The maximum number of “connectable Access Points” is Eight (8).

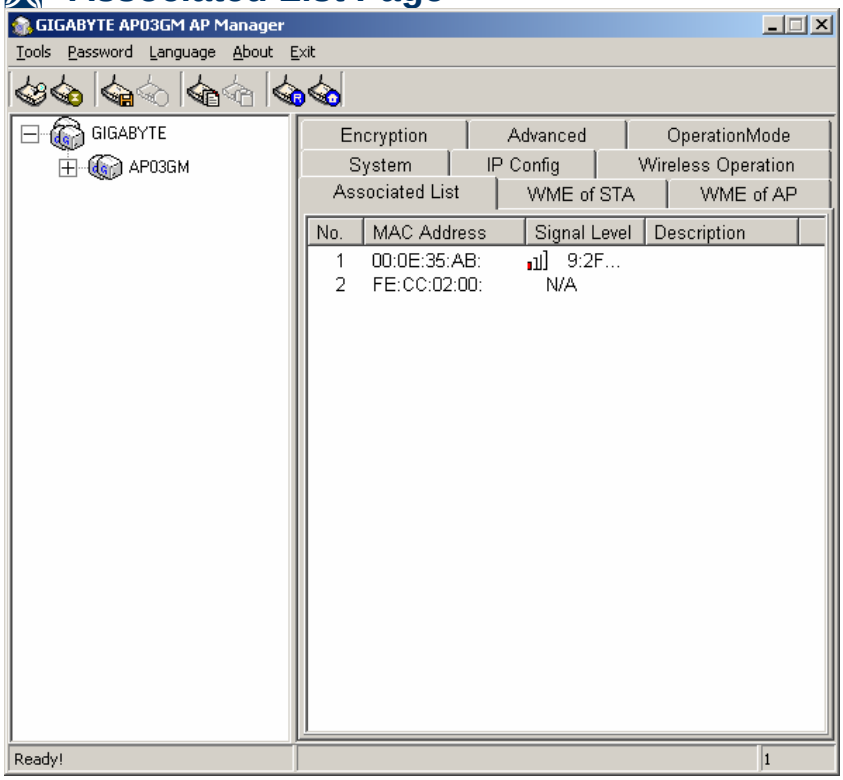


Click “**Scan**” button to display “Scan Window”. You can select which Access Point you want or choose “Select All” check box, and then click “OK” to add those MAC address into the WDS list.



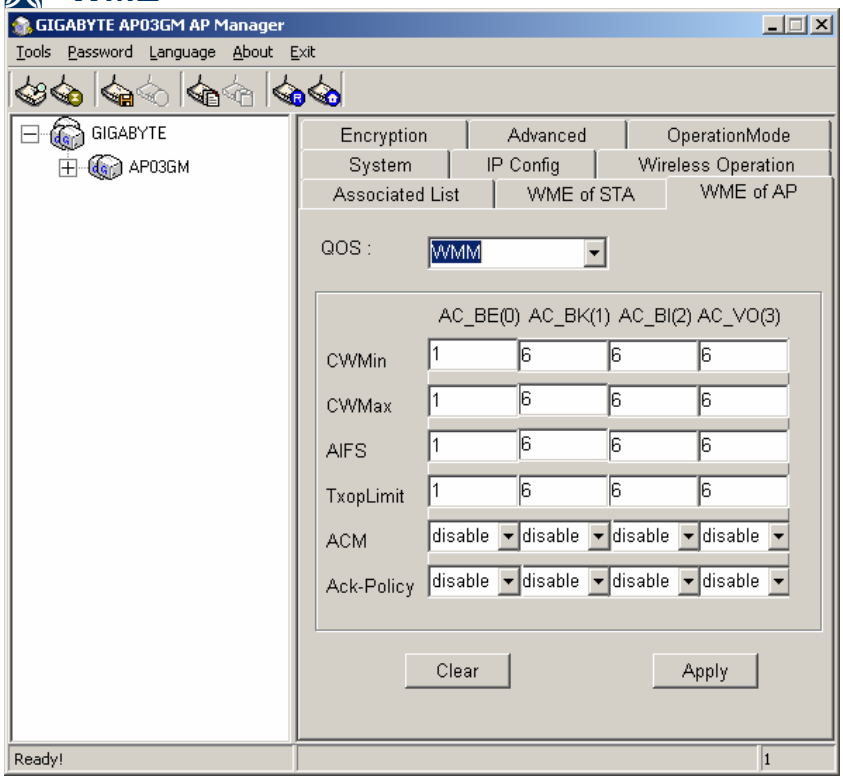
Click the “**Edit**” button to modify MAC address that you select on the WDS list. Click the “**Remove**” button to delete the MAC address from the WDS list. Or, click “**Cancel**” if you wish to cancel the operation. Finally, click the “**OK**” button to return to the “**Operation Mode**” page and click “**Apply**” button to set value into the AP.

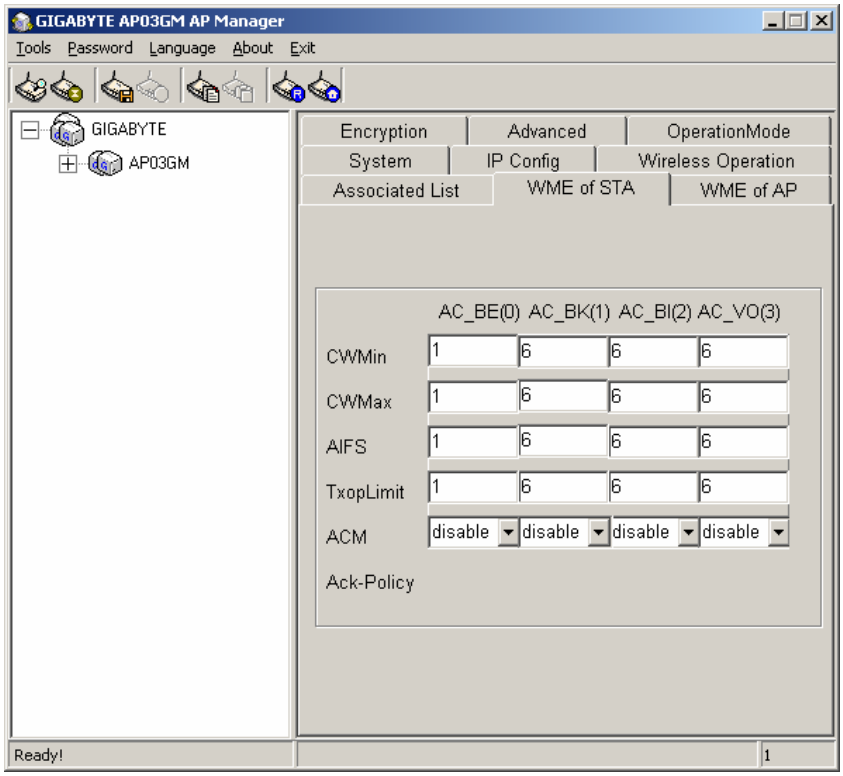
Associated List Page



From the Associated List page, the information related to the client that will connect to the Access Point may be edited. The page includes the MAC address, signal level, and description of the workstation.

WME





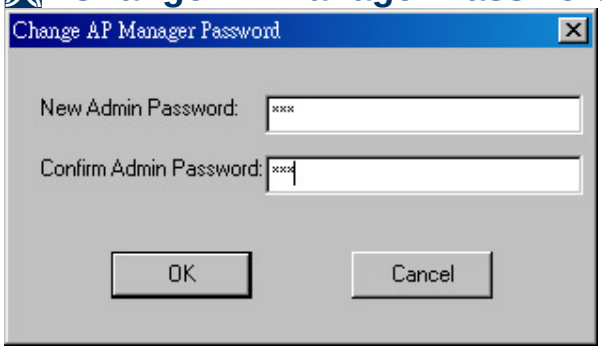
Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize

traffic and optimize the way shared network resources are allocated among different applications.

WIth this feature, users can set the data frame transmission priority for Audio, Video, Background information and Best-Effort to achieve the best performance from your applications. **Warning:** The GN-AP03GM doesn't support VLAN Tag packet format and only support IPV4 DSCP (Differentiated Services Codepoint).

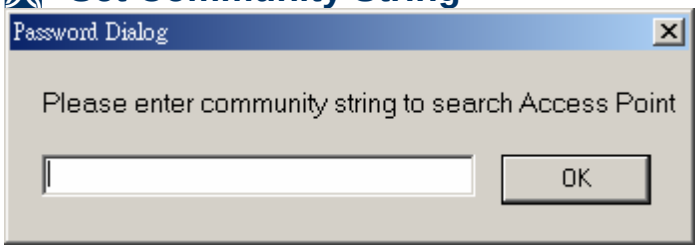
CWMin	Minimum of Contention Window
CWMax	Maximum of Contention Window
AIFS	Arbitration Inter Frame Spacing
TxopLimit	Limit time of Transmission Opportunity
ACM	Admission Control Mandatory
Ack-policy	Acknowledgment Policy (Normal ACK or No Ack)

Change AP Manager Password



Users can change the administration password of the AP Manager to prevent other users from accessing the AP Manager. On the menu bar (Password->AP Manager Password) you can invoke the password change dialogue. Please enter a new administration password, confirm it and then press **"OK"** button. You have to enter this new password the next time you wish to log into AP Manager.

Set Community String

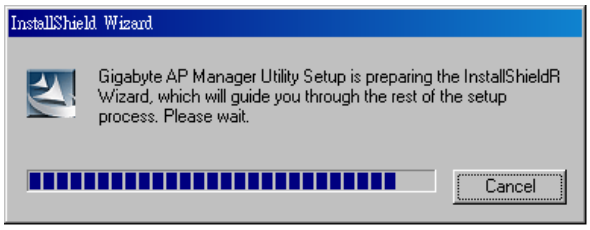


The community string defines the relationship between AP Manager and the AP. This string acts like a password to control the AP Manager's access to the AP. For a detail description, please refer to the **System** section in Chapter 3.

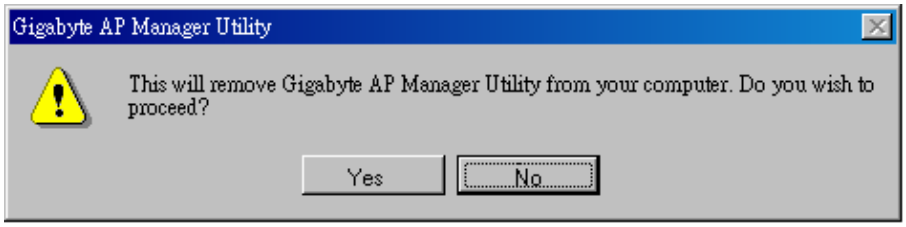
Uninstall AP Manager Utility

To uninstall AP Manager, click Windows **Start\Programs\Gigabyte AP Manager Utility\Uninstall**.

Step 1: InstallShield Wizard will appear and initialize.


InstallShield Wizard
Gigabyte AP Manager Utility Setup is preparing the InstallShieldR Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

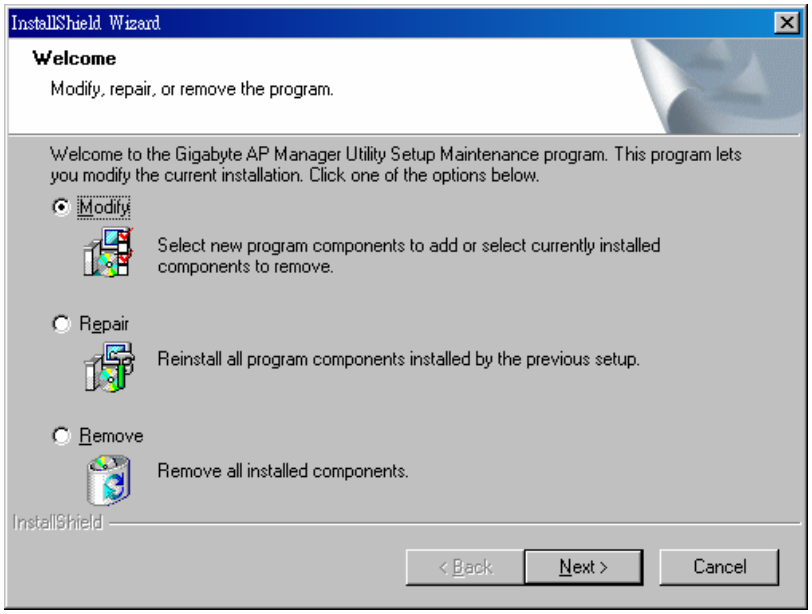
Step 2: To confirm uninstall, click **"Yes"**.


Gigabyte AP Manager Utility
This will remove Gigabyte AP Manager Utility from your computer. Do you wish to proceed?
Yes
No

Step 3: Gigabyte AP Manager Utility has been uninstalled successfully. Click **"OK"**.

If you want to modify or repair the installation or reinstall all program components, you can run the installation program again. The InstallShield Wizard will appear on the screen.

Please choose one of the options what you want (Modify, Repair, Remove) then click **"Next"**.

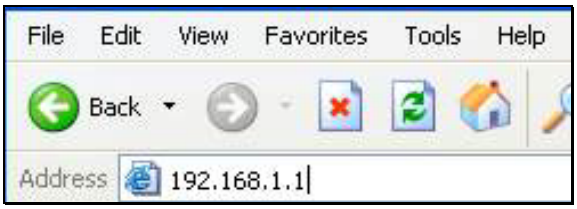

InstallShield Wizard
Welcome
Modify, repair, or remove the program.
Welcome to the Gigabyte AP Manager Utility Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.
Modify
Select new program components to add or select currently installed components to remove.
Repair
Reinstall all program components installed by the previous setup.
Remove
Remove all installed components.
InstallShield
< Back
Next >
Cancel

Chapter 4 Configuration - Using your Web-Browser

This section explains the web-based configuration method of setting up the AP with RJ45 Ethernet cables and computers connected to the AP. Any Internet Explorer 5.0 or above or Netscape Communicator 6.0 or above may be used to administer the AP.

Using Web-based configuration

Open the web-browser of your choice, and enter the local IP address of the AP into the address line of browser. (The factory default local IP is 192.168.1.1) and press **Enter**.

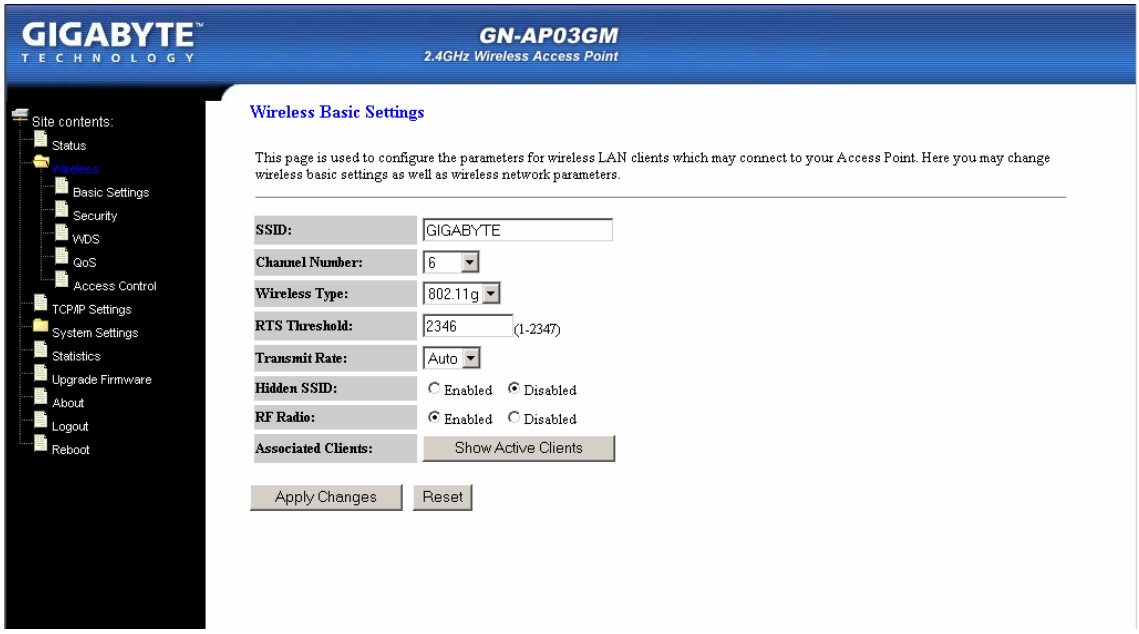


Status

You can use this status screen to view the AP's system information, current connection status and configuration.

Wireless Basic Settings

The AP will automatically detect your wireless settings. Typically, modification to the default settings is required. Changes of these settings will influence your wireless connection and performance.



- ***SSID***
  ESSID (or SSID as it is usually referred to) is the network name of the AP in the wireless network. You should set the same SSID name for all your APs to allow dynamic clients to easily roam among APs. The SSID name can be up to 32 characters in length and is case sensitive (i.e. upper case letters **"A~Z"** and lower case **"a~z"** are unique).

- ***Channel Number***
  Please choose the channel for best performance. Normally, no change is needed.

- ***Wireless Type***
  Please select your desired wireless type.

- ***RTS Threshold***
  The default value of 2346 should not be changed. However, in case of inconsistent data flow, adjustment the value to a lower number and retry. Enter a value within the range 0~2346 for the port. RTS (Request To Send) is a function, requesting permission to transmit signals. RTS is a collision avoidance method used by all 802.11b wireless networking devices. In most cases you will not need to activate or administer RTS. Generally, RTS only needs to be configured if you find yourself in an Infrastructure environment where all nodes are in range of the Access Point but may be out of range of each other.

- ***Transmit Rate***
  Select the desired data rate. The default rate is set to “Auto”.

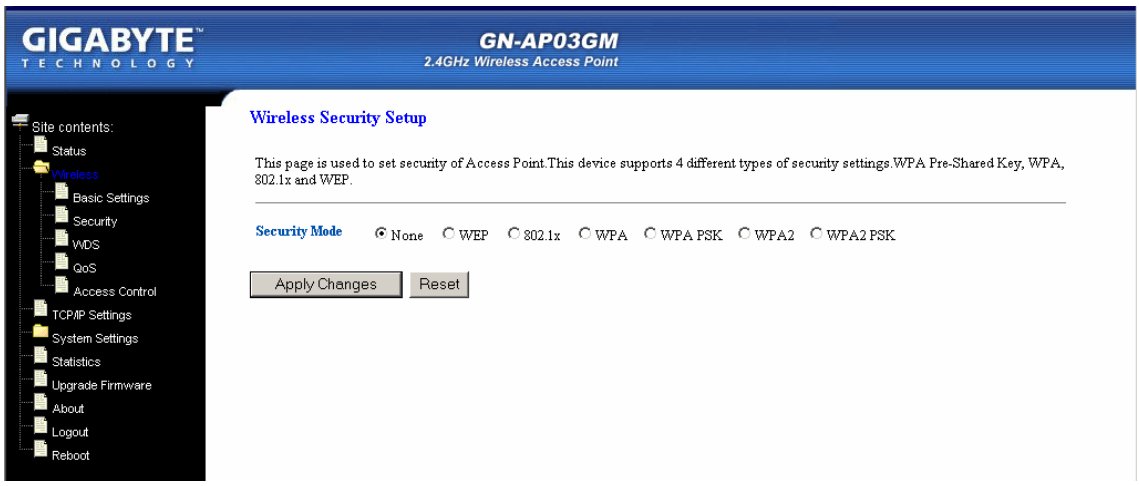
- ***Hidden ESSID***
  This setting enables you to hide ESSID name, which is needed by clients in order to connect to the AP. The default value is **“Disable”**. In this setting, ***all users are able to read your AP’s SSID name.***

- ***RF Radio***
  Enable or disable the RF Radio function.

- ***Associated Clients***
  Click **“Show Active Clients”** button to obtain the connecting users’ information.

Wireless Security Setting

Use this feature to set up the security types for the AP. Three security types are available: WEP, WPA and WPA Pre-Shared Key. If you don’t want to set up security mode, just leave the default setting: “None”.



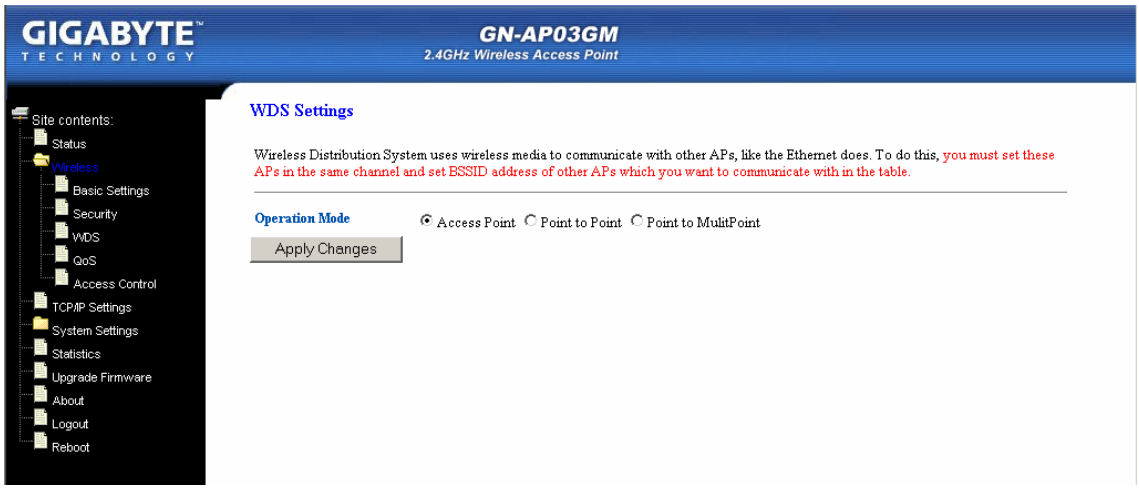
- ***WEP (Wired Equivalent Privacy)***
  WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm. The 64 bits encryption is referenced as a lower level encryption. The 128 bits is the highest level encryption.

- ***WPA/WPA2***
  If you have used Wi-Fi for a while, you may be familiar with 802.1x Authentication Protocol, which allows users to authenticate the wireless network via RADIUS server. The 802.1x Authentication Protocol is an option in standard Wi-Fi but a must for WPA. If a RADIUS server is not availiable in your environment, regardless of the needs of 802.1x, you can still use WPA. As another option for RADIUS server, WPA supports pre-shared key.

- ***WPA/WPA2 Pre-Shared Key***
  Traditional WEP had an inconvenient method to change encrypted keys. Even when you changed the encrypted keys; you still can not select all APs and wireless LAN adapter while you are changing encrypted keys.
  The manual re-keying which is necessary with WEP is a tedious manual process and is completely impractical for large organizations. After all, the instant you re-key an access point, none of the clients will be able to access it until they too are re-keyed. But with WPA, the re-keying of global encryption keys is all that is necessary. In the case of unicast traffic, the encryption key is changed after every frame using Temporary Key Integrity Protocol (TKIP). This protocol allows key changes to occur on a frame-by-frame basis and to be automatically synchronized between the access point and the wireless client. Global re-keying works by advertising the new keys to wireless clients.

WDS Settings

The Access Point supports three operation modes: “Access Point”, “Point to Point” and “Point to Multi-Point”. The default operation mode is “Access Point”.



- ***Access Point Mode***
  This allows connection of your PC to most wired networks. In most cases, no configuration setting changes are necessary.

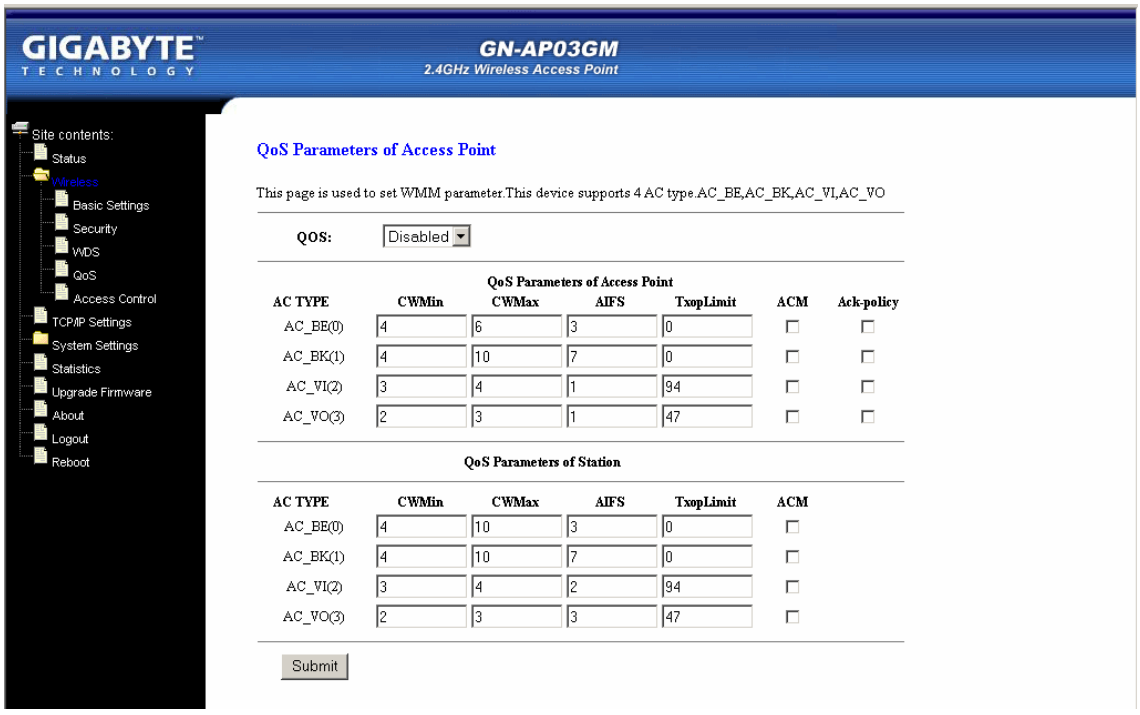
- ***Point to Point Mode***
  Only one Access Point can be assigned to connect with WDS in the “Point to Point” mode. In this WDS supported mode, the Access Point can communicate with other Gigabyte Access Point that is also set to “Point to Point” mode. You have to enter the MAC address of the host AP.

- ***Point to MultiPoint Mode***
  Up to 8 Access Points can be set to connect through WDS list in “Point to MultiPoint”. In this supported WDS mode, the Access Point can

communicate with other Gigabyte Access Points that are also set to “Point to Multi-Point” mode.

WDS technologies between AP manufactures vary, so you may not be able to establish WDS if you use APs of different brand names.

Qos Parameters of Access Point



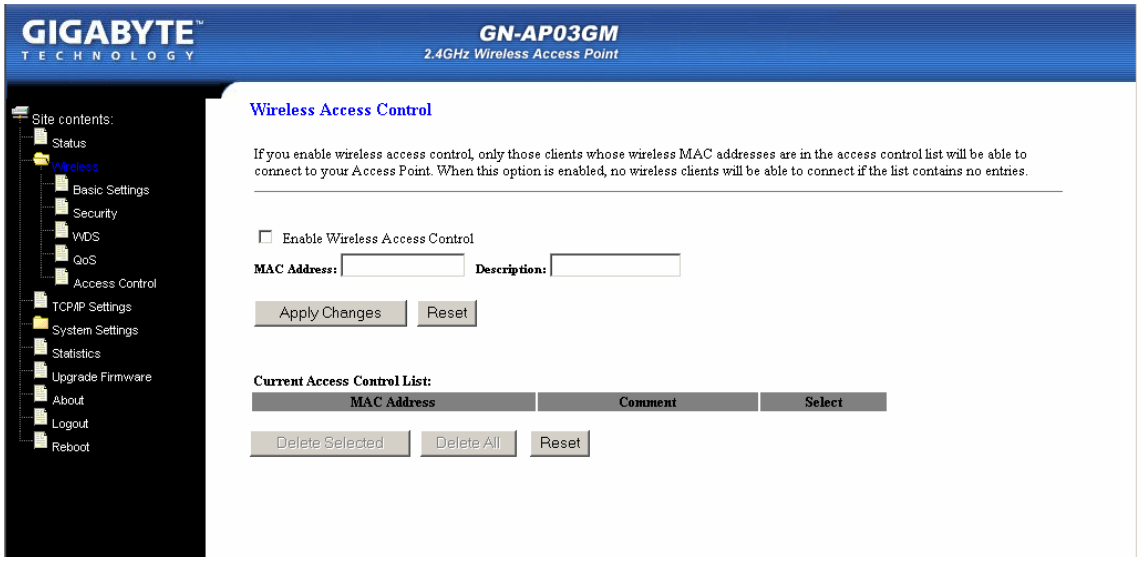
Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications.

WIth this feature, users can set the data frame transmission priority for Audio, Video, Background information and Best-Effort to achieve the best performance from your applications. **Warning:** The GN-AP03GM doesn’t support VLAN Tag packet format and only support IPV4 DSCP (Differentiated Services Codepoint).

CWMin	Minimum of Contention Window
CWMax	Maximum of Contention Window
AIFS	Arbitration Inter Frame Spacing
TxopLimit	Limit time of Transmission Opportunity
ACM	Admission Control Mandatory
Ack-policy	Acknowledgment Policy (Normal ACK or No Ack)

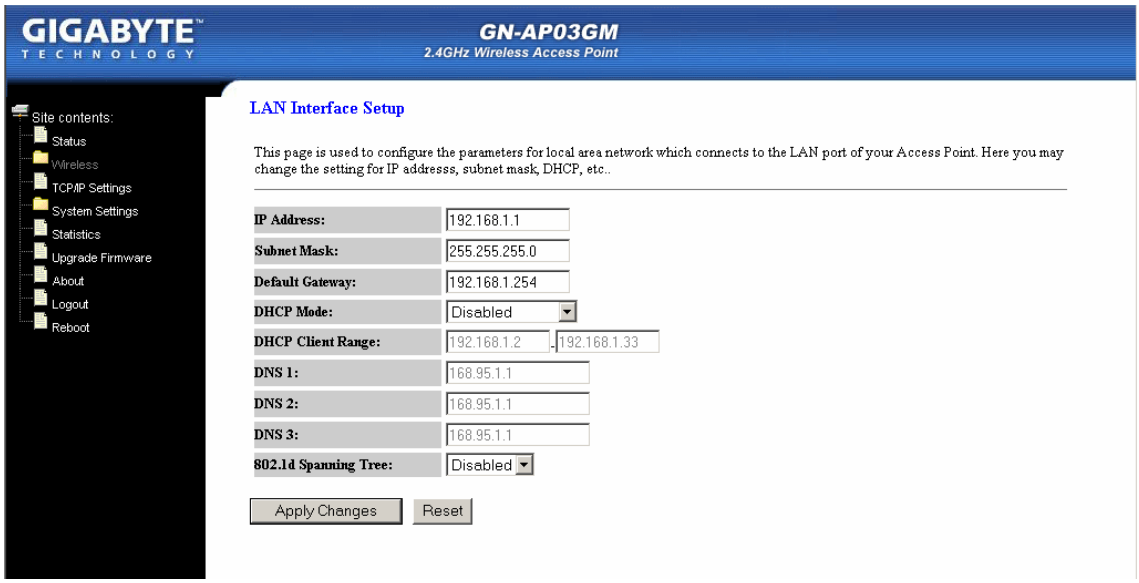
Wireless Access Control

You may specify users based on their MAC addresses that are authorized to connect to the AP. Only computers listed in the table can connect to AP when this function is enabled.



TCP/IP Settings

You may set up IP parameters for APs through TCP/IP setting screen.



- ***IP Address***
  Assign an IP address to the AP with this option. The default IP address is 192.168.1.1. Please make sure the assigned IP address is exclusive for the AP.

- ***Subnet Mask***
  Please assign a Subnet Mask for an AP. The default Subnet Mask is 255.255.255.0.

- ***Gateway***
  Please enter the IP address for the default router. The default gateway is 192.168.1.254.

After changing the IP address for AP, please change the PC's IP address (AP Manager) so that both have the same Subnet Mask. Then, click **"Find Access Point"** icon; AP Manager willl find APs on the network.

- ***DHCP Mode***
  Four (4) options are available: "Disabled", "Client Enabled" , "Server Enabled" and "Auto". The default value is "Disable".

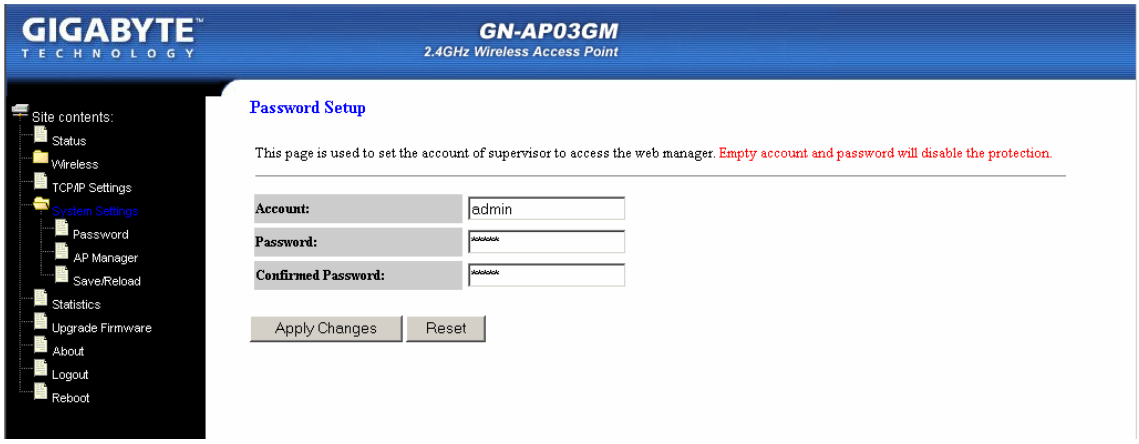
  If you want to obtain IP addresses from a DHCP server, select **"Client Enabled"**. To use an AP as a DHCP server and assign a dynamic IP address automatically on the network, select **"Server Enabled"**. If you are not sure DHCP server is available on the network and wish to use an AP as DHCP server, please select "Auto".

- ***DHCP Client Range & DNS***
  When "Server Enabled" is selected, please enter the range of your IP addresses and primary DNS. DNS information is provided by your ISP.

- ***802.1d Spanning Tree***
  When the 802.1d Spanning Tree function is enabled, the short circuit problems, loops and path redundancy among multiple APs or routers in the network can be avoided. It also comes with some overhead, and since there probably wont be many AP's or rotuers in your network, the default value is "Disable".

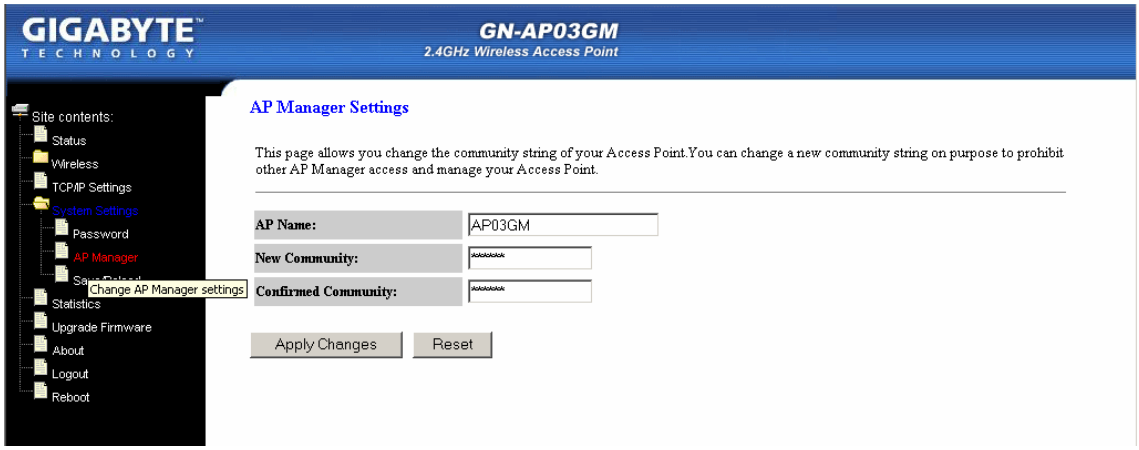
System Settings-Password Setup

Here you can set up administrator's user name and password to protect administrative access the AP. Key in a password and confirm, then press Apply Changes. Note, if you leave the password fields blank, password feature is disabled.



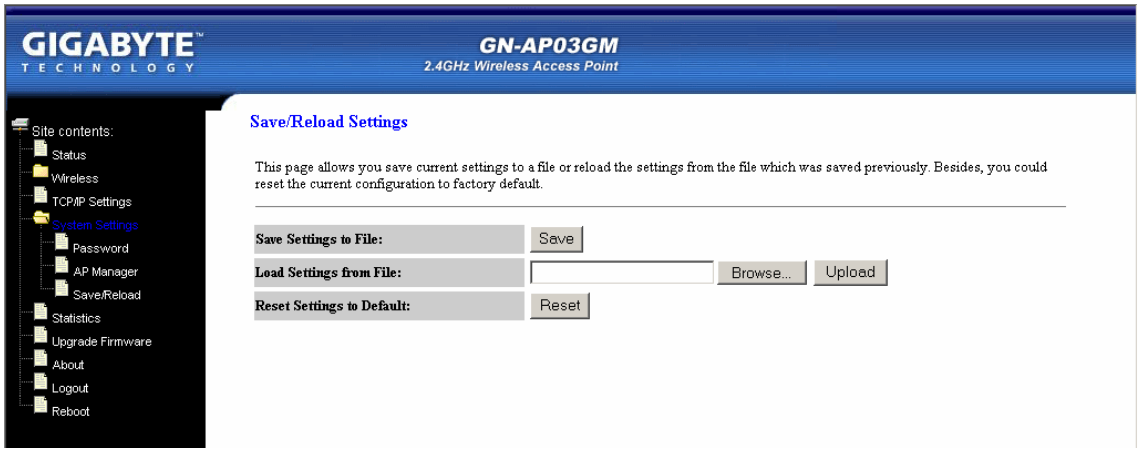
System Settings-AP Manager Settings

You may change the Community String of the AP through AP Manager Settings screen to prevent other users of AP Manager from accessing and managing the AP.



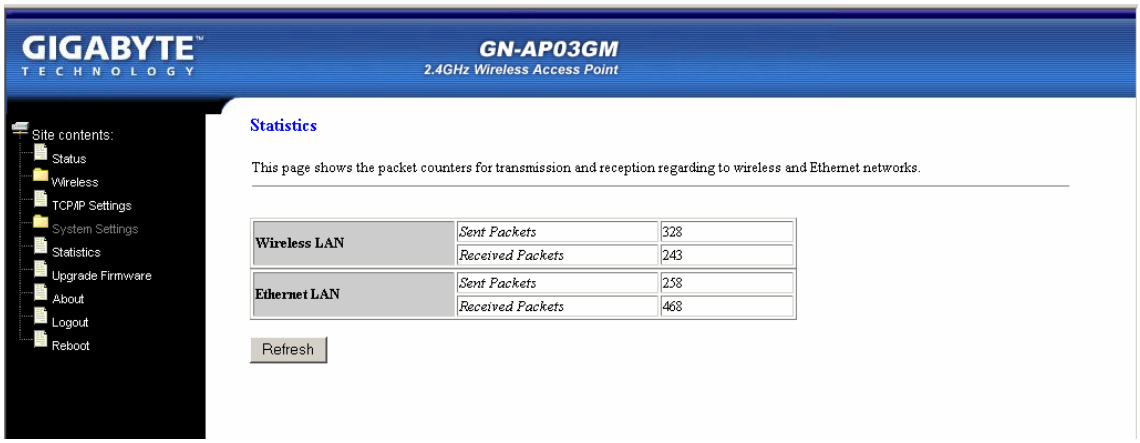
System Settings-Save/Reload Settings

You may save the current configuration as a file for restoring configuration in the future. You may press “Reset” to restore to factory default.



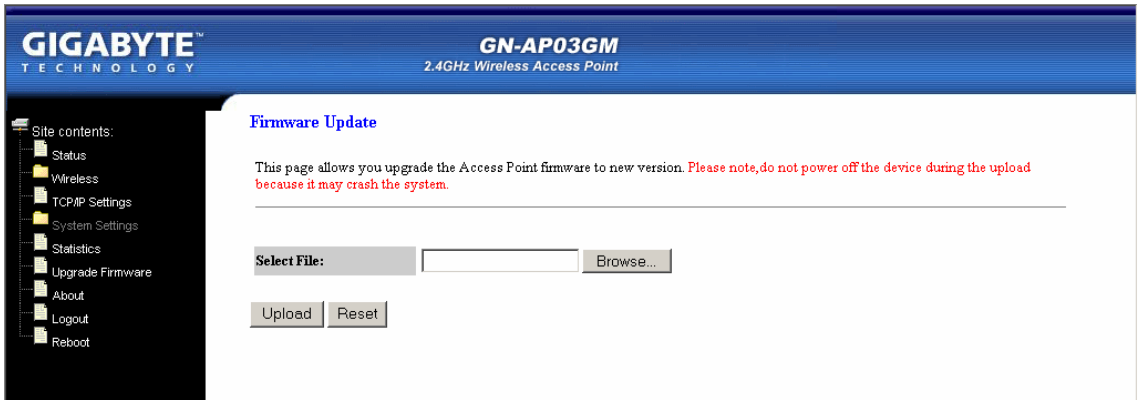
Statistics

Statistics shows you the packets flow status on the wireless LAN and Ethernet.



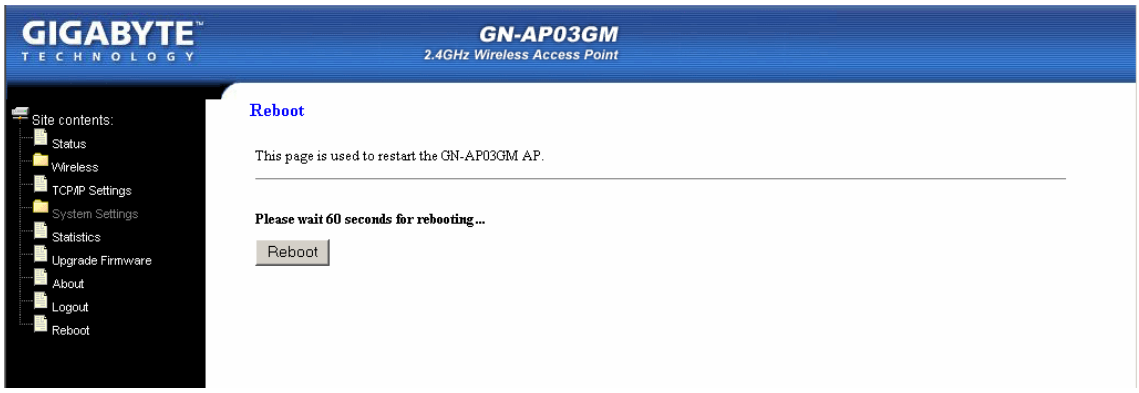
Upgrade Firmware

You can upgrade the firmware for AP with the Upgrade Firmware screen. The latest firmware version can be downloaded from Gigabyte website.



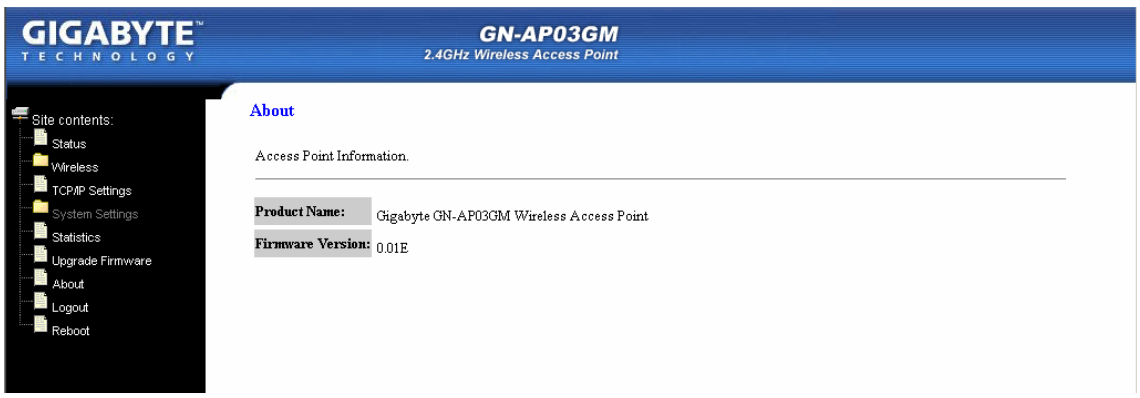
Reboot

Reboot the GN-AP03GM. The system may need up to a minute to save your settings, please allow the system to reboot itself.



About

View firmware information.



Chapter 5 Troubleshooting

This chapter gives information about troubleshooting your wireless Access Point. Read the descriptions below to help you diagnose and solve the problem.

Q: What to do if you forget your password or forget the IP address of the Access Point?

A: Please press and hold for 5 seconds the **"init"** button at the bottom of the Access Point. The Access Point will be reset to the factory default values, and the password will be restored to factory default.

Q: I am unable to connect to the Internet.

A:
1. Please confirm that the power cord is connected properly, and the Access Point's power LED is correctly lit.
2. Please confirm whether all of the settings described in this manual are correctly set.
3. Please confirm that your ADSL/Cable Modem is operating normally, and/or you have ISP service available.
4. Please confirm if your network cable is connected correctly, and the LED status is normal.

Q: I am unable to access the Access Point's Web Configuration Interface.

A:
1. Please check the Ethernet connection (RJ-45 LAN cable) between the PC and the Access Point is properly connected.
2. Make sure your computer's IP address is on the same subnet as the Access Point. (Check this by typing `ipconfig /all` from a DOS command prompt)
3. Make sure you are carefully typing the correct IP address of the router in the address bar of your web browser. The IP address of your router is the "Gateway" address you see when you run the `ipconfig /all` command.
4. Try initializing your router to factory settings.

Q: What is the IEEE 802.11b standard?

A: It is also referred to as 802.11 High Rate or Wi-Fi. It is an expansion to 802.11 that applies to wireless LAN and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. The 802.11b uses only Direct Sequence Spread Spectrum (DSSS). The 802.11b was a 1999 ratification to the origianl 802.11 standard, allowing wireless functionality comparable to Ethernet.

Q: What is WEP?

A: Wired Equivalent Privacy (WEP). A security mechanism defined within the 802.11 standard. Designed to make the link integrity of the wireless medium equal to wired cable.

Q: What is the IEEE 802.11g standard?

A: IEEE 802.11g standard specifies data rates of up to 54 Mbps in the 2.45-GHz band. It uses Orthogonal Frequency Division Multiplexing (OFDM),

which is the mandatory provisions have been made within the standard to make it inherently compatible with the well-established 802.11b standard at 11 Mbps, which uses Complementary Code Keying (CCK) modulation. Both .11g and .11b can operate at ranges of up to 300 feet.

Appendix A: Glossary

802.11e
An IEEE standard that adds Quality of Service (QoS) features and multimedia support to the existing 802.11b, 802.11g, and 802.11a wireless networks.

Access Point
An Access Point is a wired controller that sends data to the wireless NIC's installed in your network computers, and received data back from them. An Access Point is often connected to the network computer that has Internet access, or is directly connected to an ADSL or cable modem.

ADSL
Asymmetric digital subscriber line (ADSL) is a new modem technology that converts existing twisted-pair telephone lines into access paths for high-speed communication of various sorts.

Auto-MDI/MDIX
On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto- MDI/MDIX capability eliminates the need for crossover cables.

Auto-negotiate
To automatically determine the correct setting. The term is often used with communications and networking.

DHCP
The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

DSSS
Also known as "Direct Sequence Spread Spectrum," this is a variety of radio transmission methods that continuously change frequencies or signal patterns. Direct Sequence Spread Spectrum (DSSS), which is used in CDMA technology,. multiplied the data bits by a very fast, pseudo-random bet pattern (PN sequence) that "spreads" the data into a large coded stream that takes the full bandwidth of the channel.

DNS
The Domain Name System (DNS) is a distributed Internet directory service.DNS is used mostly to translate between domain names and IP addresses, and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

Dynamic IP Address
A IP address is automatically assigned to a user's AP in a TCP/IP network typically by a DHCP server.

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Gateway
A device, usually a Router, that connects hosts on a local network to other networks.

IP Address
Every PC on the Internet has a fixed identifying number, called a IP Address. A typical IP address looks like this: 216.27.61.137

MAC Address
On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's fixed hardware number.Usually written as: 01:23:45:67:89:ab

Ping (Packet Internet Groper)
A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

QoS
Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications. Without QoS, all applications running on different devices have equal opportunity to transmit data frames. That works well for data traffic from applications such as web browsers, file transfers, or e-mail but it is inadequate for multimedia applications. Voice over Internet Protocol (VoIP), video streaming, and interactive gaming are highly sensitive to latency increases and throughput reductions and require QoS. QoS extensions for 802.11 networks will be addressed in the upcoming IEEE 802.11e standard

Router
A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP network. Routers are located at gateways, the places where two or more networks connect.

SSID
The SSID is the name represents the routers and Access Point in wireless network.

Subnet Mask
A mask used to determine which subnet a IP address belongs to. An IP address has two components, the network address and the host address. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

TCP/IP
TCP/IP (Transmission Control Protocol/Internet Protocol), the suite of communications protocols used to connect hosts on the Internet.

WAN
Wide Area Network, a communication network that covers a relatively broad geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the ADSL or Cable systems, or through leased lines or satellites. To simplify it, please image network as a WAN.

WEP
WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm, as described in the IEEE 802.11 standard.

WMM™
Wi-Fi Multimedia. A group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

Appendix B: Specifications

Physical Interface

The Access Point includes one RJ-45 Ethernet LAN ports, one init button and two antenna.

Item	Contents	Description
1.	LAN Port x 1	RJ-45, Auto-sensing for 10/100M Ethernet LAN connection.
2.	Reset Button	Initial reset (Init to factory default)
3.	Antenna	Two external dipole antennas and one internal antenna.

Specifications

System	
CPU & Wireless	Realtek RTL8651B with Ralink RT2661(MAC) & RT2529 (RF)
Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b/g (Wireless)
Operating Range	Wireless - Open space: 100 – 300m; Indoor: 30 - 100m
Power Consumption	930mA @ Transmitting, 900mA @ Receiving
RF – 802.11b	
Frequency Band	2412 ~ 2484 MHz (subject to local regulation)
Modulation Technology	DSSS (Direct Sequence Spread Spectrum)
Modulation Techniques	DBPSK, DQPSK, CCK
Data Rates	11, 5.5, 2, 1 Mbps, auto fallback
Peak Output power	20 dBm @ Nominal Temp Range
Receive Sensitivity	-88 dBm @ 11 Mbps date rate at nominal temperature
Antenna	2 external dipole antennas, 1 internal antenna
RF – 802.11g (backward compatible to 802.11b)	
Frequency Band	2412 ~ 2484 MHz (subject to local regulation)
Modulation Technology	OFDM and DSSS
Modulation Techniques	64QAM, 16QAM, QPSK, BPSK, DBPSK, DQPSK, CCK
Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps, auto fallback
Output power	20 dBm @ Nominal Temp Range
Receive Sensitivity	-75 dBm @ 54 Mbps date rate at nominal temperature
Antenna	2 external dipole antennas, 1 internal antenna
Regulatory and Environmental Compliance	
EMC certification	FCC part 15 (USA)
	CE (Europe)
Temperature Range	Operating: 0 ~ 40 degree C, Storage: -20 ~ 65 degree C
Humidity	10% ~ 85% Non-condensing

GN-AP03GM AirCruiser MIMO Access Point

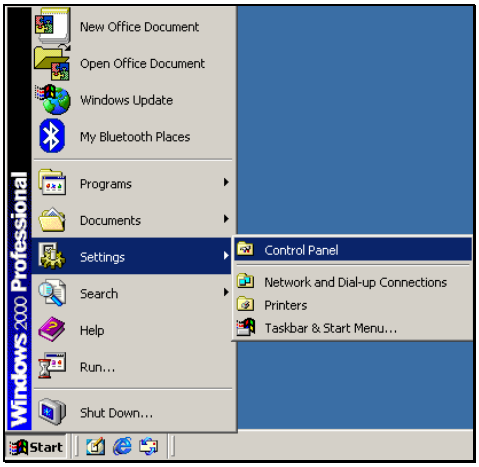
Software	
Roaming	Yes
Security	64/128 bit WEP; WPA-PSK, WPA,WPA2
Management Utility	WEB Configuration for network link
Mechanical	
Packaging	Generic, Gigabyte, private labeling optional
LED indicator	Power/Status, Wireless, LAN Port
Gross Weight	264 ± 1g
Dimension	161 mm * 152 mm * 28 mm ± 0.5mm

Appendix C: Configuration of the PCs

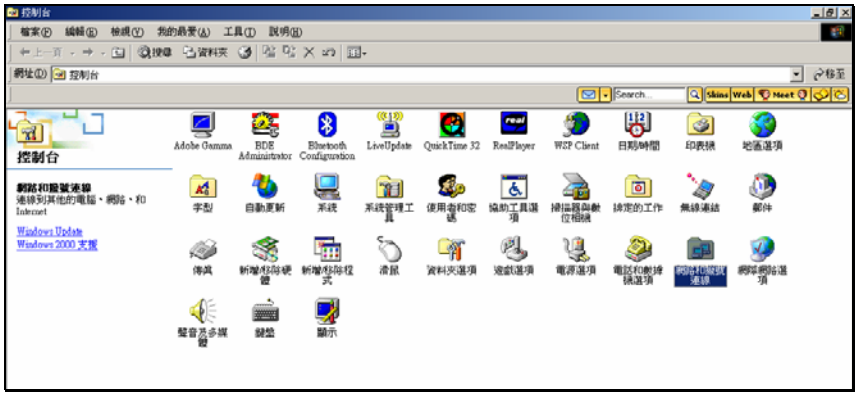
To connect to the AP, your computer needs to be located in the same Subnet as the AP. Please follow the instructions to perform the setup under the TCP/IP network environment. By default, Windows 98, *Me*, 2000 and XP already have TCP/IP installed. If you have not installed the TCP/IP communication Protocol, please install it now, and then select your operating system for the setup.

TCP/IP Settings Under Windows 2000

Step 1. Click the **Start** button, select **Settings** and then click the **Control Panel** icon.

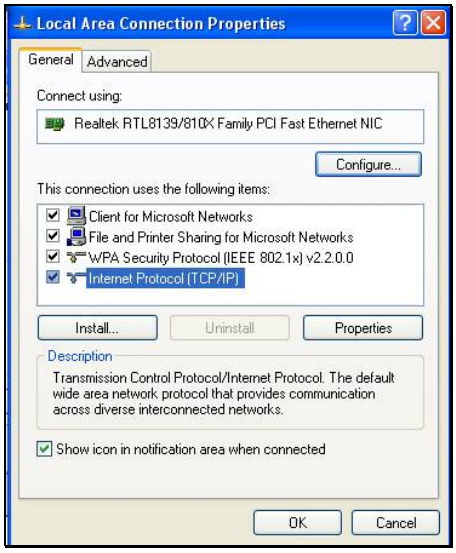


Step 2. Double-click the **Network and Dial-up Connection** icon.

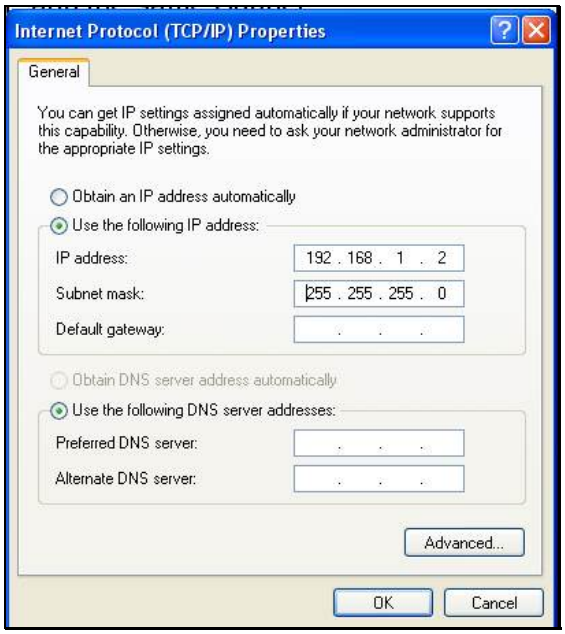


Step 3. Double-click the **"LAN CONNECTION"** and click the **"Properties"** button.

Step 4. The **"Local Area Connection Properties"** dialog box will appear. Verify that the Internet Protocol (TCP/IP) item is checked. Then double-click on **Internet Protocol (TCP/IP)**.

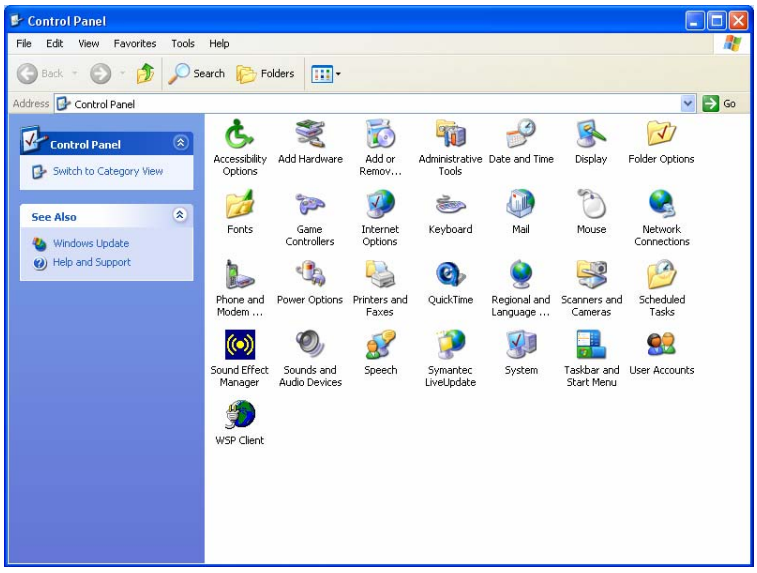


Step 5. Assign the static IP address used by the AP and the same Subnet Mask to the computer (For example, IP address is 192.168.1.2 and Subnet Mask is 255.255.255.0), click the “OK” button to return to Local Area Connection Properties. Click the “OK” button again to complete the PC configuration.

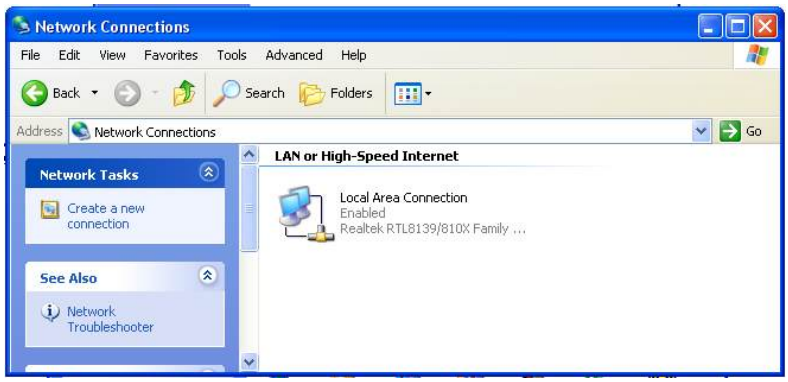

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

TCP/IP Settings under Windows XP

Step 1. Click the **“Start”** in the desktop of the Windows to select **“Settings”**, and then select the **“Control Panel”**.

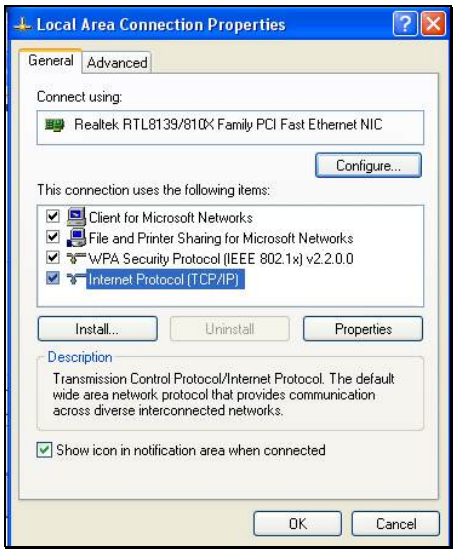


Step 2. Double-click the **"Network Connections"** icon.

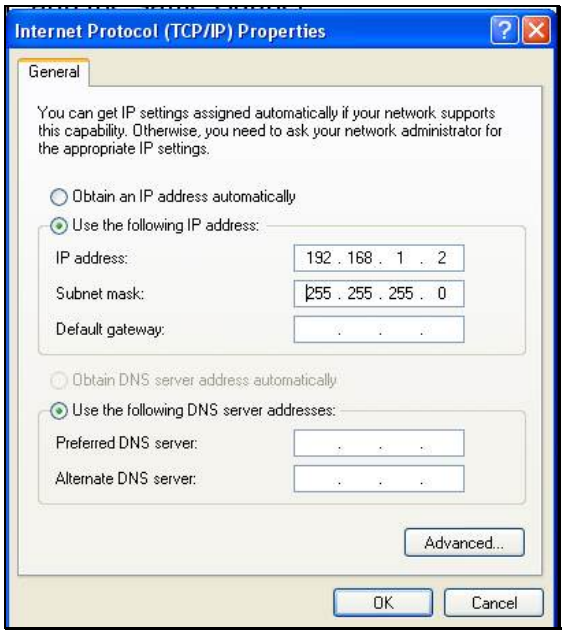


Step 3. Double-click the **"LAN CONNECTION"** and click the **"Properties"** button.

Step 4. The **"Local Area Connection Properties"** dialog box will appear. Verify that the Internet Protocol (TCP/IP) item is checked. And then double-click on **"Internet Protocol (TCP/IP)"** item.


Local Area Connection Properties
General Advanced
Connect using:
Realtek RTL8139/810X Family PCI Fast Ethernet NIC
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
WPA Security Protocol (IEEE 802.1x) v2.2.0.0
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

Step 5. Assign the static IP address used by the AP and the same Subnet Mask to the computer (For example, IP address is192.168.1.2 and Subnet Mask is 255.255.255.0), click the “OK” button to return to **“Local Area Connection Properties”**. Click the “OK” button again to complete the PC configuration.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Limited Warranty Statement

1-Year Warranty

GIGABYTE makes warranty to the original consumer/purchaser that the product is free from defects in materials and workmanship from the time of purchase and for a limited time of one year thereafter. This warranty is null and void if the product is damaged in the process of being installed or improperly used.

GIGABYTE may replace or repair the product with either new or reconditioned parts. Repaired or replaced products will be returned to you at the same revision level as received or higher at GIGABYTE's option. GIGABYTE reserves the right to replace discounted products with an equivalent generation product.

KEEP THIS STUB FOR YOUR PURCHASING RECORD

Customer:	
Phone No:	
Address:	
Email:	
Model:	
Serial:	
Date of Purchase:	
Place of Purchase:	
Reseller:	
Distributor:	

Customer Satisfaction

GIGA-BYTE TECHNOLOGY CO., LTD.

No.6, Bau Chiang Road, Hsin-Tien, Taipei Hsien, Taiwan
Phone No: 886-2-89124888
Fax: 886-2-89124007
http://www.gigabyte.com.tw